PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-141895
(43)Date of publication of application : 17.05.2002
(51)Int.Cl. H04L 9/08
G06F 15/00
G06F 17/60
G09C 1/00
H04L 9/32
H04N 7/167
H04N 7/173
(21)Application number : 2000-334183 (71)Applicant : SONY CORP
SONY COMPUTER ENTERTAINMENT INC
(22)Date of filing : 01.11.2000 (72)Inventor : YOSHINO KENJI
ISHIBASHI YOSHITO
AKISHITA TORU
SHIRAI TAIZO
OKA MAKOTO
YOSHIMORI MASAHARU

(54) SYSTEM AND METHOD FOR DISTRIBUTING CONTENTS

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a contents distributing system for surely and efficiently billing for distributed contents, etc.
SOLUTION: A shop server transmits an enciphering contents key by a form to be decoded through the use of the storage key of a user device to the user device on condition that the charging is completed concerning the contents purchase request of the user unit. A user device authenticating server(DAS) for managing a contents distribution performs a processing by which a contents key KpDAS(Kc) enciphered by the open key of DAS is changed into a contents key KpDEV(Kc) enciphered by the open key KpDEV of the user device. The shop server transmits the changes contents key to the user device on condition that the charging processing is completed with respect to the contents purchase request.

LEGAL STATUS [Date of request for examination] 05.03.2007
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against eaminer's decision of rejection]
[Date of extinction of right]

* NOTICES *
JPO and INPIT **are not responsible for any damages** caused **by the use of this translation.**
1.This document has been translated by computer. So the translation may not reflect the original precisely.

2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.
CLAIMS
[Claim(s)]
[Claim 1] While receiving the contents purchase demand from the user machine (DEV) which transmits a contents purchase demand to a shop server, and said user machine The shop server which manages the encryption contents enciphered with the contents key Kc, and the encryption contents key which cannot be decoded with the storing key of said user machine (SHOP), It has the key or ** which uses said encryption contents key as the encryption contents key which can be decoded with the storing key of said user machine, or the user machine authentication server (DAS) which obtains and performs processing. It is contingent [on the accounting based on the contents purchase with said user machine having been completed]. The contents distribution system characterized by considering as the configuration which provides said user machine with the encryption contents key which can be decoded with the storing key of the user machine which said user machine authentication server generated from said shop server.
[Claim 2] The encryption contents key which cannot be decoded with the storing key of said user machine It is the encryption contents key KpDAS (Kc) enciphered with the public key KpDAS of said user machine authentication server (DAS). It obtains in the key or ** which said user machine authentication server (DAS) performs. Processing Decode said encryption contents key KpDAS (Kc) with the private key KsDAS of said user machine authentication server (DAS), and the contents key Kc is acquired. The contents distribution system according to claim 1 characterized by being the processing which furthermore re-enciphers with the public key KpDEV of said user machine (DEV), and generates the encryption contents key KpDEV (Kc).
[Claim 3] Said user machine authentication server receives the encryption contents key which cannot be decoded with the storing key of said user machine to said user machine. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server The contents distribution system according to claim 1 characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].
[Claim 4] Said user machine authentication server receives the encryption contents key which cannot be decoded with the storing key of said user machine from said shop server. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server The contents distribution system according to claim 1 characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].
[Claim 5] Said contents distribution system has further the distribution server which distributes encryption contents to said user machine. Said shop server It has the configuration which transmits a contents distribution demand for the contents purchase demand from said user machine to said distribution server according to reception. Said

distribution server The contents distribution system according to claim 1 characterized by having the configuration which performs processing which distributes encryption contents to said user machine according to the contents distribution demand from said shop server.
[Claim 6] The contents purchase requested data which said user machine generates and is transmitted to said shop server The shop ID as an identifier of the shop which is a requested data transmission place, the transaction ID as a contents dealings identifier It is constituted as data which include the electronic signature of a user machine while having the content ID as a contents identifier for a purchase demand. Said shop server While checking data alteration existence by performing signature verification of said contents purchase requested data Based on this contents purchase requested data, a new entry is added to a shop management database. The contents distribution system according to claim 1 characterized by having the configuration which sets up the status information which shows the processing situation over this additional entry, and manages processing sequence transition at this shop based on said status information.
[Claim 7] Said user machine authentication server is the contents distribution system according to claim 1 characterized by to have the configuration which obtains in the key or ** from either of said user machine or said shop server, adds a new entry to a user machine authentication server management database according to reception of a demand, sets up the status information which shows the processing situation over this additional entry, and manages the processing sequence transition by this user machine authentication server based on said status information.
[Claim 8] They are a shop server and the user machine authentication server which performs distribution management of the contents dealt with between user machines. Obtain in the key or ** received from said shop server or said user machine, and it responds to receipt of a demand. The contents key which is an encryption key of contents dealt with between a shop server and a user machine It has the key changed into the encryption contents key which can be decoded with the storing key of said user machine from the encryption contents key enciphered in the mode which cannot be decoded with the storing key of said user machine, **, or the configuration which obtains and performs processing. the electronic signature of said shop server which obtains said user machine authentication server in said key or **, and is contained during a demand -- and The user machine authentication server characterized by having the configuration which obtains in said key or ** a condition [having verified the electronic signature of said user machine, having obtained in said key or ** by this verification and the justification of a demand having been checked], and performs processing.
[Claim 9] It is the shop server which offers the contents key applied to decode of encryption contents to a user machine. The encryption contents key which enciphered the contents key which is an encryption key of contents in the mode which cannot be decoded with the storing key of said user machine is managed, and it is contingent [on completion of the accounting based on the contents purchase demand from said user machine]. It obtains in the key or ** of an encryption contents key enciphered in the mode which the user machine authentication server (DAS) which manages contents distribution cannot decode with the storing key of said user machine. By processing The shop server characterized by having the configuration which performs processing which

transmits the encryption contents key which can be decoded with the storing key of said user machine to generate to said user machine.
[Claim 10] Said shop server is a shop server according to claim 9 characterized by being a configuration containing the distribution server of encryption contents.
[Claim 11] It is the contents playback device which generates the purchase demand of contents, transmits to a shop server, and performs regeneration of contents. The encryption contents key data which can be decoded with the storing key of the key or ** which the user machine authentication server (DAS) which performs distribution management of contents performs, or said contents playback device which obtains and is generated by processing are received through a shop server. Signature verification of the shop server contained in the this encryption contents key data to receive and a user machine authentication server (DAS) is performed, and it is contingent [on it having been checked that there is no data alteration]. The contents playback device characterized by having the configuration which takes out and decodes an encryption contents key from the received encryption contents key data, and performs acquisition processing of a contents key.
[Claim 12] In the step which transmits a contents purchase demand from a user machine (DEV) to a shop server (SHOP), and a shop server (SHOP) In the step which receives the contents purchase demand from said user machine, and a user machine authentication server (DAS) The key changed into the encryption contents key which can be decoded with the storing key of said user machine from the encryption contents key which cannot be decoded with the storing key of said user machine, **, or the step which obtains and performs processing, It is contingent [on the accounting based on the contents purchase with said user machine having been completed in said shop server]. The contents distribution approach characterized by having the step which provides said user machine with the encryption contents key which can be decoded with the storing key of the user machine which said user machine authentication server generated from said shop server.
[Claim 13] The encryption contents key which cannot be decoded with the storing key of said user machine It is the encryption contents key KpDAS (Kc) enciphered with the public key KpDAS of said user machine authentication server (DAS). It obtains in the key or ** which said user machine authentication server (DAS) performs. Processing Decode said encryption contents key KpDAS (Kc) with the private key KsDAS of said user machine authentication server (DAS), and the contents key Kc is acquired. The contents distribution approach according to claim 12 characterized by being the processing which furthermore re-enciphers with the public key KpDEV of said user machine (DEV), and generates the encryption contents key KpDEV (Kc).
[Claim 14] Said user machine authentication server receives the encryption contents key which cannot be decoded with the storing key of said user machine to said user machine. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server The contents distribution approach according to claim 12 characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].

[Claim 15] Said user machine authentication server receives the encryption contents key which cannot be decoded with the storing key of said user machine from said shop server. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server The contents distribution approach according to claim 12 characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].
[Claim 16] The contents purchase requested data which said user machine generates and is transmitted to said shop server The shop ID as an identifier of the shop which is a requested data transmission place, the transaction ID as a contents dealings identifier It is constituted as data which include the electronic signature of a user machine while having the content ID as a contents identifier for a purchase demand. Said shop server While checking data alteration existence by performing signature verification of said contents purchase requested data Based on this contents purchase requested data, a new entry is added to a shop management database. The contents distribution approach according to claim 12 characterized by setting up the status information which shows the processing situation over this additional entry, and managing processing sequence transition at this shop based on said status information.
[Claim 17] Said user machine authentication server is the contents distribution approach according to claim 12 characterized by obtaining in the key or ** from either of said user machine or said shop server, adding a new entry to a user machine authentication server management database according to reception of a demand, setting up the status information which shows the processing situation over this additional entry, and managing the processing sequence transition by this user machine authentication server based on said status information.
[Claim 18] It is the program offer medium which offers the computer program which makes the message distribution processing of a contents key perform on computer system. Said computer program The step which receives the encryption contents key which can be decoded with the storing key of the user machine which the user machine uthentication server (DAS) which manages contents distribution generates, The step which performs accounting based on the contents purchase demand from said user machine, The program offer medium characterized by having the step which transmits the encryption contents key which can be decoded with the storing key of a user machine to said user machine a condition [completion of said accounting].
DETAILED DESCRIPTION
[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to a contents distribution system and the contents distribution approach. Furthermore, it is related with the contents distribution system and the contents distribution approach of having improved in the detail the entity which performs contents offer service, and the security in the contents dealings between the user machines who perform contents reception and a management configuration. In addition, a system is the logical set configuration of two or more equipments, and it does not restrict to what has equipment of each configuration in the same case.

[0002]
[Description of the Prior Art] Circulation through networks, such as the Internet of various software data (these are hereafter called contents (Content)), such as a game program, voice data, image data, and a document preparation program, prospers these days. Moreover, goods dealing, settlement-of-accounts processing, etc. through networks, such as on-line shopping, bank settlement of accounts, and ticket sale, prosper.
[0003] In the data communication through such a network, it is common to take the data transfer configuration which transmits required information, namely, took security into consideration after checking that a data source and a data receiving side were the regular candidates for data transceiver mutually. The technique of realizing the security configuration in the case of data transfer has transfer data encryption processing, the signature processing to data, etc.
[0004] Encryption data can be returned to available decode data (plaintext) by decryption processing in a predetermined procedure. The data encryption and the decryption approach of using an encryption key for encryption processing of such information, and using a decryption key for decryption processing are well learned from the former.
[0005] Although there are various classes of the modes of the data encryption and the decryption approach using an encryption key and a decryption key, there is a method called the so-called public key cryptosystem as the one example. A public key cryptosystem is taken as the private key with which one key is kept as what is different in the key of an addresser and an addressee, and an unspecified user keeps another side secret as an usable public key. For example, use a data encryption key as a public key, and let a decode key be a private key. Or it is used in a mode, such as using an authentication child generation key as a private key, and using an authentication child verification key as a public key.
[0006] Since one specific person should just have a private key with the need of keeping it secret by the public key cryptosystem unlike the so-called common key encryptosystem-ized method using a key common to encryption and a decryption, it is advantageous in management of a key. However, as compared with a common key encryptosystem-ized method, the processing data rate of a public key cryptosystem is slow, and they are used. [for an object with little amount of data, such as delivery of a private key and a digital signature,] [many] A RSA (Rivest-Shamir-Adleman) code is one of the typical things of a public key cryptosystem. This uses the difficulty of the processing of the product of the two big prime factors (for example, 150 figures) which carries out factorization in prime numbers using the product of the two very big prime factors (for example, 150 figures).
[0007] In the public key cryptosystem, many approaches of using the certificate proving whether the public key which is the configuration made usable and distributes a public key to many and unspecified persons is just, and the so-called public key certificate are used. For example, the pair of a public key and a private key is generated, and User A sends the generated public key to a certificate authority, and receives a public key certificate from a certificate authority. Generally User A exhibits a public key certificate. An unspecified user receives a public key through a predetermined procedure from a public key certificate, enciphers a document etc., and sends to User A. User A is the

system of decoding an encryption document etc. using a private key. Moreover, User A is a system which a signature is attached to a document etc. using a private key, and an unspecified user receives a public key through a predetermined procedure from a public key certificate, and verifies the signature.
[0008] A public key certificate is a certificate which the certificate authority or issue station (CA:Certificate Authority or IA:Issuer Authority) in a public key cryptosystem publishes, and when a user submits self ID, a public key, etc. to a certificate authority, it is a certificate with which a certificate authority side adds information, such as ID of a certificate authority, and an expiration date, adds the signature by the certificate authority further, and is created.
[0009] A public key certificate includes electronic signature in the algorithm used for the version number of a certificate, the serial number of the certificate which an issue station assigns to a certificate user, and electronic signature and a parameter, the identifier of a certificate authority, the expiration date of a certificate, a certificate user's identifier (user ID), and a certificate user's public key list.
[0010] Electronic signature is data which generated the hash value with the application of the Hash Function to a certificate user's whole public key in the algorithm used for the version number of a certificate, the serial number of the certificate which a certificate authority assigns to a certificate user, and electronic signature and the parameter, the identifier of a certificate authority, the expiration date of a certificate, and a certificate user's identifier list, and were generated using the private key of a certificate authority to the hash value.
[0011] On the other hand, in case this public key certificate is used, using the public key of the certificate authority which self holds, a user verifies the electronic signature of the public key certificate concerned, after he succeeds in verification of electronic signature, he picks out a public key from a public key certificate, and uses the public key concerned. Therefore, all the users using a public key certificate need to hold the public key of a common certificate authority.
[0012]
[Problem(s) to be Solved by the Invention] In the data transmitting system by the public key cryptosystem using the public key certificate of the above certificate authority issue, the contents distribution shop which distributes contents, for example enciphers the contents for distribution based on a user's public key, and transmits them to a user. The user machine which received the encryption data from a contents distribution shop performs decode of encryption contents with the self private key corresponding to a self public key.
[0013] However, the contents distribution shop where a license holder with the right of distribution of contents or the contents manufacturer with the copyright of contents performs offer service to the user of contents in actual contents dealings is a different existence in many cases, and about whether it has the right of contents use with the just user who has received contents, the contents distribution shop is distributing contents in many cases, without checking. That is, contents may be unfairly used or sold by the user without the just right of use.
[0014] Moreover, in the above dealings gestalten, although the dealings accompanied by the suitable charge of contents use are materialized in between 2 persons of the contents distribution shop which is the vender of contents, and the user machine which

is a contents user, acquisition of the charge of a license accompanying the contents dealings between a shop and a user in a license holder with the right of distribution of contents or the contents manufacturer with the copyright of contents is not guaranteed. It is a general dealings gestalt that check the distribution cost of contents and a license holder or a contents manufacturer is provided with the charge of a license based on self-assessment by self-assessment of a contents distribution shop from a shop in the present condition.

[0015] The license holder which has the right of distribution of contents with such a contents dealings gestalt, or the contents manufacturer with the copyright of contents has not grasped the stereo of contents dealings, and did not have a means to check whether contents are circulating justly under the exact right of use.

[0016] The contents distribution system and the contents distribution approach of this invention having been made in view of the trouble in the above contents dealings, having made grasp certainly possible in the license holder which has the right of distribution of contents for the stereo of the contents dealings between the contents distribution shops and the users who perform distribution service of contents, or the contents manufacturer with the copyright of contents, and having carried out as the configuration which performs contents distribution under management of the just right of contents use provide.

[0017]

[Means for Solving the Problem] While the 1st side face of this invention receives the contents purchase demand from the user machine (DEV) which transmits a contents purchase demand to a shop server, and said user machine The shop server which manages the encryption contents enciphered with the contents key Kc, and the encryption contents key which cannot be decoded with the storing key of said user machine (SHOP), It has the key or ** which uses said encryption contents key as the encryption contents key which can be decoded with the storing key of said user machine, or the user machine authentication server (DAS) which obtains and performs processing. It is contingent [on the accounting based on the contents purchase with said user machine having been completed]. It is in the contents distribution system characterized by considering as the configuration which provides said user machine with the encryption contents key which can be decoded with the storing key of the user machine which said user machine authentication server generated from said shop server.

[0018] The contents distribution system of this invention sets like 1 operative condition. Furthermore, the encryption contents key which cannot be decoded with the storing key of said user machine It is the encryption contents key KpDAS (Kc) enciphered with the public key KpDAS of said user machine authentication server (DAS). It obtains in the key or ** which said user machine authentication server (DAS) performs. Processing Decode said encryption contents key KpDAS (Kc) with the private key KsDAS of said user machine authentication server (DAS), and the contents key Kc is acquired. It is characterized by being the processing which furthermore re-enciphers with the public key KpDEV of said user machine (DEV), and generates the encryption contents key KpDEV (Kc).

[0019] The contents distribution system of this invention sets like 1 operative condition. Furthermore, said user machine authentication server The encryption contents key

which cannot be decoded with the storing key of said user machine to said user machine is received. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server It is characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].
[0020] The contents distribution system of this invention sets like 1 operative condition. Furthermore, said user machine authentication server From said shop server, the encryption contents key which cannot be decoded with the storing key of said user machine is received. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server It is characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].
[0021] The contents distribution system of this invention sets like 1 operative condition. Furthermore, said contents distribution system It has the distribution server which distributes encryption contents to said user machine. Furthermore, said shop server It has the configuration which transmits a contents distribution demand for the contents purchase demand from said user machine to said distribution server according to reception. Said distribution server It is characterized by having the configuration which performs processing which distributes encryption contents to said user machine according to the contents distribution demand from said shop server.
[0022] Furthermore, the contents purchase requested data which the contents distribution system of this invention sets like 1 operative condition, and said user machine generates, and is transmitted to said shop server The shop ID as an identifier of the shop which is a requested data transmission place, the transaction ID as a contents dealings identifier It is constituted as data which include the electronic signature of a user machine while having the content ID as a contents identifier for a purchase demand. Said shop server While checking data alteration existence by performing signature verification of said contents purchase requested data Based on this contents purchase requested data, a new entry is added to a shop management database. The status information which shows the processing situation over this additional entry is set up, and it is characterized by having the configuration which manages processing sequence transition at this shop based on said status information.
[0023] The contents distribution system of this invention sets like 1 operative condition. Furthermore, said user machine authentication server Obtain in the key or ** from either of said user machine or said shop server, and it responds to reception of a demand. A new entry is added to a user machine authentication server management database, the status information which shows the processing situation over this additional entry is set up, and it is characterized by having the configuration which manages the processing sequence transition by this user machine authentication server based on said status information.
[0024] Furthermore, the 2nd side face of this invention is a shop server and a user machine authentication server which performs distribution management of the contents

dealt with between user machines. Obtain in the key or ** received from said shop server or said user machine, and it responds to receipt of a demand. The contents key which is an encryption key of contents dealt with between a shop server and a user machine It has the key changed into the encryption contents key which can be decoded with the storing key of said user machine from the encryption contents key enciphered in the mode which cannot be decoded with the storing key of said user machine, **, or the configuration which obtains and performs processing. the electronic signature of said shop server which obtains said user machine authentication server in said key or **, and is contained during a demand -- and The electronic signature of said user machine is verified and it is in the user machine authentication server characterized by having the configuration which obtains in said key or ** a condition [having obtained in said key or ** by this verification, and the justification of a demand having been checked], and performs processing.

[0025] Furthermore, the 3rd side face of this invention is a shop server which offers the contents key applied to decode of encryption contents to a user machine. The encryption contents key which enciphered the contents key which is an encryption key of contents in the mode which cannot be decoded with the storing key of said user machine is managed, and it is contingent [on completion of the accounting based on the contents purchase demand from said user machine]. It obtains in the key or ** of an encryption contents key enciphered in the mode which the user machine authentication server (DAS) which manages contents distribution cannot decode with the storing key of said user machine. By processing It is in the shop server characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to generate to said user machine.

[0026] Furthermore, the shop server of this invention sets like 1 operative condition, and said shop server is characterized by being a configuration containing the distribution server of encryption contents.

[0027] Furthermore, the 4th side face of this invention is a contents playback device which generates the purchase demand of contents, transmits to a shop server, and performs regeneration of contents. The encryption contents key data which can be decoded with the storing key of the key or ** which the user machine authentication server (DAS) which performs distribution management of contents performs, or said contents playback device which obtains and is generated by processing are received through a shop server. Signature verification of the shop server contained in the this encryption contents key data to receive and a user machine authentication server (DAS) is performed, and it is contingent [on it having been checked that there is no data alteration]. It is in the contents playback device characterized by having the configuration which takes out and decodes an encryption contents key from the received encryption contents key data, and performs acquisition processing of a contents key.

[0028] Furthermore, the 5th side face of this invention is set to the step which transmits a contents purchase demand from a user machine (DEV) to a shop server (SHOP), and a shop server (SHOP). In the step which receives the contents purchase demand from said user machine, and a user machine authentication server (DAS) The key changed into the encryption contents key which can be decoded with the storing key of said user

machine from the encryption contents key which cannot be decoded with the storing key of said user machine, **, or the step which obtains and performs processing, It is contingent [on the accounting based on the contents purchase with said user machine having been completed in said shop server]. It is in the contents distribution approach characterized by having the step which provides said user machine with the encryption contents key which can be decoded with the storing key of the user machine which said user machine authentication server generated from said shop server.

[0029] The contents distribution approach of this invention sets like 1 operative condition. Furthermore, the encryption contents key which cannot be decoded with the storing key of said user machine It is the encryption contents key KpDAS (Kc) enciphered with the public key KpDAS of said user machine authentication server (DAS). It obtains in the key or ** which said user machine authentication server (DAS) performs. Processing Decode said encryption contents key KpDAS (Kc) with the private key KsDAS of said user machine authentication server (DAS), and the contents key Kc is acquired. It is characterized by being the processing which furthermore re-enciphers with the public key KpDEV of said user machine (DEV), and generates the encryption contents key KpDEV (Kc).

[0030] The contents distribution approach of this invention sets like 1 operative condition. Furthermore, said user machine authentication server The encryption contents key which cannot be decoded with the storing key of said user machine to said user machine is received. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server It is characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].

[0031] The contents distribution approach of this invention sets like 1 operative condition. Furthermore, said user machine authentication server From said shop server, the encryption contents key which cannot be decoded with the storing key of said user machine is received. The encryption contents key which can be decoded with the storing key of a key, **, or the user machine that obtains and is generated by processing is transmitted to said shop server. Said shop server It is characterized by having the configuration which performs processing which transmits the encryption contents key which can be decoded with the storing key of said user machine to said user machine a condition [completion of said accounting].

[0032] Furthermore, the contents purchase requested data which the contents distribution approach of this invention sets like 1 operative condition, and said user machine generates, and is transmitted to said shop server The shop ID as an identifier of the shop which is a requested data transmission place, the transaction ID as a contents dealings identifier It is constituted as data which include the electronic signature of a user machine while having the content ID as a contents identifier for a purchase demand. Said shop server While checking data alteration existence by performing signature verification of said contents purchase requested data Based on this contents purchase requested data, a new entry is added to a shop management database, the status information which shows the processing situation over this

additional entry is set up, and it is characterized by managing processing sequence transition at this shop based on said status information.
[0033] The contents distribution approach of this invention sets like 1 operative condition. Furthermore, said user machine authentication server Obtain in the key or ** from either of said user machine or said shop server, and it responds to reception of a demand. A new entry is added to a user machine authentication server management database, the status information which shows the processing situation over this additional entry is set up, and it is characterized by managing the processing sequence transition by this user machine authentication server based on said status information.
[0034] Furthermore, the 6th side face of this invention is a program offer medium which offers the computer program which makes the message distribution processing of a contents key perform on computer system. The step which receives the encryption contents key which can decode said computer program with the storing key of the user machine which the user machine authentication server (DAS) which manages contents distribution generates, The step which performs accounting based on the contents purchase demand from said user machine, It is in the program offer medium characterized by having the step which transmits the encryption contents key which can be decoded with the storing key of a user machine to said user machine a condition [completion of said accounting].
[0035] In addition, the program offer medium concerning the 6th side face of this invention is a medium which offers a computer program in a computer-readable format to the general purpose computer system which can perform various program codes, for example. Especially the gestalten, such as transmission media, such as record media, such as CD, and FD, MO, or a network, are not limited for a medium.
[0036] Such a program offer medium defines the collaboration-relation on the structure of the computer program and offer medium for realizing the function of a computer program predetermined in a computer system top, or a function. If it puts in another way, by installing a computer program in computer system through this offer medium, on computer system, a collaboration-operation is demonstrated and the same operation effectiveness as other side faces of this invention can be acquired.
[0037] The purpose, the description, and advantage of further others of this invention will become [rather than] clear by detailed explanation based on the example and the drawing to attach of this invention mentioned later.
[0038]
[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained to a detail, referring to a drawing. In addition, explanation is performed according to the following items.
1. Key or ** of Encryption Contents Key, or Contents Distribution Management 1.1. System Configuration Obtain and According to Processing : Public Key Certificate or Attribute Certificate Use Configuration [0039] Which Recorded Contents Distribution Management 4. Attribute Data Based on Contents Distribution Model 3. Log Collection Server Using Modification 1.3. Basic Contents Distribution Model 22. Electronic Ticket of Basic Contents Distribution Model 11.2. Basic Contents Distribution Model 1
[Example] [1. The key or ** of an encryption contents key, or contents distribution management] obtain and according to processing

[-- 1.1. -- system configuration: -- drawing which explains the outline of one example of the contents distribution system of this invention and the contents distribution approach to basic contents distribution model 1] drawing 1 is shown. In addition, a system is the logical set configuration of two or more equipments, and it does not restrict to what has equipment of each configuration in the same case.
[0040] The contents distribution system of drawing 1 uses as the main component the user machine authentication server (DAS:Device Authentication Server) 300 which functions as the user machine (DEVICE) 200 which receives the contents distribution from the shop server (SHOP) 100 and the shop server 100 which performs distribution service of the contents to a user machine, and a management server which performs still more nearly just contents dealings management. In addition, two or more each components shown in drawing 1 exist, and information is transmitted [although the shop server 100, the user machine 200 and every one user machine authentication server 300 are shown / in an actual contents dealings configuration / for every contents dealings] with the configuration of drawing 1 , and received by various roots. Drawing 1 shows the data flow in one contents dealings.
[0041] (Shop server) The configuration of the shop server 100 of the contents distribution system of drawing 1 is shown in drawing 2 . The shop server 100 has the contents database 110 which stored the encryption contents key KpDAS (Kc) which enciphered the contents key Kc as Kc (Content) which is encryption contents data which enciphered the contents used as the candidate for dealings by the contents key by public key:KpDAS of a user machine authentication server (DAS:Device Authentication Server). In addition, the content ID which is a contents identifier, respectively is added, and Kc (Content) which is encryption contents data has an identifiable configuration based on content ID, as shown also in drawing.
[0042] The shop server 100 has the purchase management database 120 which matches and manages an identifier, a contents identifier, etc. of contents dealings management data, for example, the user machine of a contents sale place, further. Furthermore, it has the control means 130 which performs communications processing with extract processing of the distribution contents from the contents database 110, generation processing of the dealings data registered to the purchase management database 120 accompanying dealings, the user machine 200, and the user machine authentication server 300, data cipher processing further for each communications processing, etc.
[0043] The data configuration of the purchase management database 120 is shown in drawing 3 . Shop processing No. as an identification number which carries out internal generation in case, as for the purchase management database 120, a shop server performs processing according to contents dealings, The device ID which is the identifier of a user machine which published the contents purchase request The transaction ID as a contents dealings identifier which carries out generation issue with a user vessel in case the contents dealings between a user machine and a shop are performed It has each information on the status which shows the status of the contents dealings processing in the content ID and the shop server which are the identifier of the contents for dealings. The status is updated according to advance of two or more processings accompanying dealings of contents, although the latter part explains to a detail.

[0044] As a control means 130 is shown in drawing 2 , it also has a function as a cipher-processing means and a communications processing means, and a control means 130 is constituted by the computer which stored for example, the code processing program and the communication link processing program. The key data used in cipher processing performed in the cipher-processing means of a control means 130 are stored in the storage means inside a control means secure one. As code problem data, such as a cryptographic key which the shop server 100 stores, there is a public key KpCA of the certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private key:KsSHOP of a shop server, public key certificate Cert_SHOP of a shop server, and a public key certificate.
[0045] The example of a configuration of a control means 130 is shown in drawing 4 . The configuration of a control means 130 is explained. A control section 131 is constituted by the arithmetic and program control (CPU:Central Processing Unit) which performs various processing programs, and controls processing of each configuration part of the control means of drawing 4 . ROM (Read only Memory)132 is the memory which memorized programs, such as IPL (Initial Program Loading). RAM (Random Access Memory)133 is used as the storing field of executive programs, such as the program which a control section 131 performs, for example, a database manager, a code processing program, and a communications program, and a work area in each [these] program manipulation.
[0046] A display 134 has display means, such as a liquid crystal display and CRT, and displays the data at the time of various program executions, for example, the user data of a contents distribution place etc., under control of a control section 131. The input section 135 has a keyboard and pointing devices, such as a mouse, and outputs the command from each [these] input device, and a data input to a control section 131. As for HDD (Hard Disk Drive)136, various data are stored in programs, such as a database manager, a code processing program, and a communications program, and a pan.
[0047] Drive 137 has the function which controls access to various record media, such as semiconductor memory, such as magneto-optic disks, such as optical disks, such as HD (Hard Disk), and magnetic disks, such as FD (Floppy Disk), CD-ROM (Compact Disk ROM), and a mini disc, ROM, and a flash memory. Various record media, such as a magnetic disk, memorize a program, data, etc. A network interface 138 functions as an interface of the communication link through cables, such as the Internet and the telephone line, and wireless.
[0048] The shop server 100 performs various cipher processing accompanying the contents dealings between the user machine 200 which is the candidate for dealings of contents, or the user machine authentication server 300, authentication processing, etc. in the control means 130 with the configuration mentioned above.
[0049] (User machine authentication server) The configuration of the user machine authentication server (DAS) 300 is shown in drawing 5 . A user machine authentication server has the license management database 320. The data configuration of the license management database 320 is shown in drawing 6 . User machine authentication server processing No. as a processing identifier in which a license management database carries out internal generation according to the processing to which a user machine authentication server (DAS) performs at the time of contents dealings, The device ID which is the identifier of a user machine which published the contents purchase request

The transaction ID as a contents dealings identifier which carries out generation issue with a user vessel in case contents dealings are performed The shop ID which is the identifier of the content ID which is the identifier of the contents for dealings, and the shop server which performs contents dealings It has each information on the status which shows the status of the contents dealings processing in shop processing No. which is a processing identifier in the shop which a shop publishes, and a user machine authentication server (DAS). The status is [0050] updated according to advance of two or more processings accompanying dealings of contents although the latter part explains to a detail. The user machine authentication server (DAS) 300 has the control means 330 which performs communications processing with the user machine 200 and the shop server 100, data cipher processing further for each communications processing, etc. A control means 330 has a function as a cipher-processing means and a communications processing means as well as the control means of the shop server explained previously. The configuration is the same as the configuration explained using drawing 4 . The key data used in cipher processing performed in the cipher-processing means of a control means 330 are stored in the storage means inside a control means secure one. As code problem data, such as a cryptographic key which the user machine authentication server (DAS) 300 stores, there is a public key KpCA of the certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private key:KsDAS of a user machine authentication server (DAS), public key certificate Cert_DAS of a user machine authentication server (DAS), and a public key certificate.

[0051] (User machine) The configuration of the user machine 200 is shown in drawing 7 . A user machine is for example, a contents playback device which performs use of the contents which performed and purchased the purchase of contents, i.e., contents playback, and activation, and has the purchase management database 220. The data configuration of the purchase management database 220 is shown in drawing 8 . In case a purchase management database performs contents dealings, it has further each information on the status which shows the status of the contents dealings processing in the shop ID which is the identifier of the content ID which is the transaction ID as a contents dealings identifier which carries out generation issue with a user vessel, and the identifier of the contents for dealings, and the shop server which performs contents dealings, and a user machine, and the device ID which is the instrument identification child of a user machine. The status is updated according to advance of two or more processings accompanying dealings of contents, although the latter part explains to a detail.

[0052] The user machine 200 has the control means 230 which performs communications processing with the shop server 100 and the user machine authentication server 300, data cipher processing further for each communications processing, etc. A control means 230 has a function as a cipher-processing means and a communications processing means as well as the control means of the shop server explained previously. The configuration is the same as the configuration explained using drawing 4 . The key data used in cipher processing performed in the cipher-processing means of a control means 230 are stored in the storage means inside a control means secure one. There is a preservation key Ksto applied as an encryption key at the time of storing the public key KpCA and contents of a certificate authority (CA:Certificate

Authority) as a public key certificate issue station which is the issue engine of private key:KsDEV of a user machine, public key certificate Cert_DEV of a user machine, and a public key certificate in storage means, such as a user machine, for example, a hard disk etc., as code problem data, such as a cryptographic key which the user machine 200 stores.

[0053] The [public key certificate] above-mentioned shop server (SHOP) 100, the user machine (DEVICE) 200, and the public key certificate that the user machine authentication server (DAS:Device Authentication Server) 300 holds are explained using drawing 9 .

[0054] A third person (CA:Certificate Authority), i.e., an issue station, proves that it is the public key with which a user with the just public key to be used has a public key certificate in processing of the mutual recognition between 2 persons who perform the transmission and reception of code data which used the public key, or data transmission and reception etc. The outline of a format of a public key certificate is shown in drawing 9 (a).

[0055] A version (version) shows the version of a certificate format. The serial number of a certificate is a serial number (Serial Number), and is the serial number of the public key certificate set up by the public key certificate issue station (CA). A signature algorithm identifier and an algorithm parameter (Signature algorithm Identifier algorithm parameter) are the fields which record the signature algorithm and parameter of a public key certificate. In addition, when there are an elliptic curve cryptosystem and RSA and the elliptic curve cryptosystem is applied as a signature algorithm, a parameter and key length are recorded, and key length is recorded when RSA is applied. The identifier of an issue office is the field where the publisher of a public key certificate, i.e., the name of a public key certificate issue office (CA), is recorded in an identifiable format (Distinguished Name). The initiation time and termination time whose expiration date (validity) of a certificate is an expiration date of a certificate are recorded. The identifier of the authentication candidate whose user name (ID) of a public key certificate is a user is recorded. Specifically, they are ID of a user machine, a service provision subject's ID, etc. A user public key (subject Public Key Info algorithm subject Public key) is the field which stores the key algorithm as a user's public key information, and the key information itself. The signature which an issue station attaches is electronic signature performed to the data of a public key certificate using the private key of a public key certificate issue station (CA), and the user of a public key certificate can verify using the public key of a public key certificate issue station (CA), and can check the alteration existence of a public key certificate.

[0056] The generation method of electronic signature using a public key cryptosystem is explained using drawing 10 . The processing shown in drawing 10 is the generation processing flow of the electronic signature data which used EC-DSA (Elliptic Curve Digital SignatureAlgorithm) (IEEE P1363/D3). In addition, the example which used the elliptic curve cryptosystem (Elliptic Curve Cryptography (hereafter referred to as ECC)) as public key encryption here is explained. in addition, in the data processor of this invention, it is also possible to use RSA cryptograph (Rivest, Shamir, Adleman), such as etc. (ANSI X9.31), in the same public key cryptosystem besides an elliptic curve cryptosystem.

[0057] Each step of drawing 10 is explained. It sets to step S1 and is the multiplier (elliptic curve: let the base point on an elliptic curve, and r into the order of G, and let Ks be a private key (0<Ks<r) for four a3+27b2!=0 (mod p) and G.) of an elliptic curve about the characteristic, and a and b in p. Step S2 The hash value of Message M is calculated by setting, and it considers as f=Hash (M).
[0058] Here, how to calculate a hash value using a Hash Function is explained. A Hash Function is a function which considers a message as an input, compresses this into the data of predetermined bit length, and is outputted as a hash value. It is difficult for a Hash Function to predict an input from a hash value (output), and when 1 bit of the data inputted into the Hash Function changes, discovering different input data which many bits of a hash value change and has the same hash value has the difficult description. As a Hash Function, MD4, MD5, SHA-1, etc. may be used and DES-CBC may be used. In this case, MAC (check value: it is equivalent to ICV) used as a final output value serves as a hash value.
[0059] Continuously, at step S3, a random number u (0<u<r) is generated and the coordinate V (Xv, Yv) which doubled the base point u by step S4 is calculated. In addition, the addition on an elliptic curve and 2 double ** are defined as follows.
[0060]
[Equation 1] When P= (Xa, Ya), Q= (Xb, Yb), and R=(Xc, Yc) =P+Q, it is Xc=lambda 2-2 XaYc=lambda x(Xa-Xc)-Yalambda=(3 (Xa) 2+a)/(2Ya) [0061] at the time (2 double **) of Xc=lambda 2-Xa-XbYc=lambda x(Xa-Xc)-Yalambda=(Yb-Ya)/(Xb-Xa)P=Q at the time of P!=Q (addition). u times of Point G are calculated using these (although a rate is slow, it carries out as follows as the most intelligible operation approach.). G, 2xG, and 4xG .. is calculated and 2 ixG (value which 2-double-**(ed) G i times (bit position when counting i from LSB of u)) corresponding to the place carries out binary number expansion of the u, and 1 stands is added.
[0062] At step S5, c=Xvmod r is calculated and it judges whether this value is set to 0 at step S6, if it is not 0, d=[(f+cKs) /u] mod r will be calculated at step S7, it judges whether d is 0 at step S8, and if d is not 0, c and d will be outputted as electronic signature data by step S9. If r is assumed to be the die length of 160 bit length, electronic signature data serve as 320 bit length.
[0063] In step S6, when c is 0, it returns to step S3 and a new random number is regenerated. Similarly, when d is 0 at step S8, it returns to step S3 and a random number is regenerated.
[0064] Next, the verification approach of electronic signature using a public key cryptosystem is explained using drawing 11 . step S11 -- M -- let the multiplier (elliptic curve: y2=x3+ax+b) of an elliptic curve, and G as the base point on an elliptic curve, and let [a message and p / the characteristic, and a and b] the order of G, G, and KsxG be public keys (0<Ks<r) for r. It verifies whether the electronic signature data c and d fill 0<c<r and 0<d<r with step S12. When this is being filled, at step S13, the hash value of Message M is calculated and it considers as f=Hash (M). Next, h= 1-/d mod r is calculated at step S14, and it is h1=fh at step S15. mod r, h2=ch mod r is calculated.
[0065] In step S16, point P=(Xp, Yp) =h1xG+h2 and KsxG are calculated using h1 and h2 which were already calculated. Since the electronic signature verification person knows a public key G and KsxG, he can do count of the scalar multiple of the point on an elliptic curve like step S4 of drawing 10 . And Point P judges whether it is an infinite

point at step S17, and if it is not an infinite point, it will progress to step S18 (the judgment of an infinite point will be able to be performed at step S16 in fact.). That is, if addition of P= (X, Y) and Q= (X, -Y) is performed, lambda cannot be calculated but it will have become clear that P+Q is an infinite point. Xp mod r is calculated at step S18, and it compares with the electronic signature data c. Finally, when this value is in agreement, it progresses to step S19 and electronic signature judges with the right.

[0066] When electronic signature is judged to be the right, it turns out that data were not altered but the person holding the private key corresponding to a public key generated electronic signature.

[0067] In step S12, when the electronic signature data c or d do not fill 0<c<r and 0<d<r, it progresses to step S20. Moreover, in step S17, also when Point P is an infinite point, it progresses to step S20. In step S18, also when the value of Xp mod r is not in agreement with the electronic signature data c, it progresses to step S20 further again.

[0068] In step S20, when judged with electronic signature not being right, it turns out that those who data are altered or hold the private key corresponding to a public key did not generate electronic signature.

[0069] The signature of an issue station is made by the public key certificate, and it has become it by signature verification by the public key user with the configuration which can check the alteration of a certificate. Return explanation is continued to drawing 9 . Drawing 9 (b) is public key certificate:Cert_DEV of the user machine stored in a user machine, and stores the public key KpDEV of the user machine ID and a user machine. Drawing 9 (c) is public key certificate:Cert_SHOP of the shop server stored in a shop server, and stores the public key KpSHOP of Shop ID and a shop server. Drawing 9 (d) is public key certificate:Cert_DAS of the user machine authentication server stored in a user machine authentication server, and stores user machine authentication server ID and the public key KpDAS of a user machine authentication server. Thus, a user machine, a shop server, and a user machine authentication server hold a public key certificate, respectively.

[0070] [Contents purchase processing], next the processing whose return and user machine purchase and use contents for drawing 1 from a shop server are explained. Processing advances in order of (20) from the number (1) of drawing 1 . The detail of processing is explained to each numerical order. In addition, although this example has described what performed mutual recognition processing ((1), (7), (11)) in the communication link between entities, you may omit if needed.

[0071] (1) The user machine 200 which is going to purchase mutual recognition contents from the shop server 100 performs mutual recognition processing between shop servers. Between two means to perform data transmission and reception, it is performed that a partner checks mutually whether you are a right data communication person, and performs required data transfer mutually after that. Check processing of whether a partner is a right data communication person is mutual recognition processing. The configuration which performs encryption processing by using as a share key the session key which performed generation of a session key and was generated at the time of mutual recognition processing, and performs data transmission is one desirable data transfer method.

[0072] The mutual recognition approach using a common key encryption system is explained using drawing 12 . In drawing 12 , although DES is used as a common key

encryption system, as long as it is the same common key encryption system, any are sufficient.
[0073] First, B generates the random number Rb which is 64 bits, and transmits ID (b) which is Rb and self ID to A. A which received this newly generates the 64-bit random number Ra, in order of Ra, Rb, and ID (b), Key Kab is used for it in the CBC mode of DES, it enciphers data, and returns them to B.
[0074] B which received this decrypts received data with Key Kab. First, the decryption approach of received data decrypts a cipher E1 with Key Kab, and obtains a random number Ra. Next, a cipher E2 is decrypted with Key Kab, the exclusive OR of E1 is carried out to the result, and Rb is obtained. Finally, a cipher E3 is decrypted with Key Kab, the exclusive OR of E2 is carried out to the result, and ID (b) is obtained. In this way, Rb and ID (b) verify whether it is in agreement with what B transmitted among Ra, Rb(s), and ID (b) which were obtained. When it passes in this verification, B attests A as a just thing.
[0075] Next, B generates the session key (Session Key (hereafter referred to as Kses)) used after authentication (a random number is used for a generation method). And in order of Rb, Ra, and Kses, in the CBC mode of DES, Key Kab is used, it enciphers, and A is returned.
[0076] A which received this decrypts received data with Key Kab. Since the decryption approach of received data is the same as that of decryption processing of B, a detail is omitted here. In this way, Rb and Ra verify whether it is in agreement with what A transmitted among Rb(s), Ra, and Kses(es) which were obtained. When it passes in this verification, A attests B as a just thing. After attesting the partner of each other, the session key Kses is used as a common key for the secret communication after authentication.
[0077] In addition, when injustice and an inequality are found on the occasion of verification of received data, processing is interrupted as that in which mutual recognition failed.
[0078] Next, the mutual recognition approach using the elliptic curve cryptosystem of the 160 bit length which is a public key cryptosystem is explained using drawing 13 . In drawing 13 , although ECC is used as a public key cryptosystem, as long as it is the public key cryptosystem same as mentioned above, any are sufficient. Moreover, key size may not be 160 bits, either. In drawing 13 , first, B generates the 64-bit random number Rb, and transmits to A. A which received this newly generates the 64-bit random number Ra and the random number Ak smaller than Characteristic p. And point Av=AkxG which doubled the base point G Ak is calculated, electronic signature A.Sig to Ra, Rb, and Av (X coordinate and Y coordinate) is generated, and B is returned with the public key certificate of A. Here, since 64 bits, and the X coordinate and Y coordinate of Av are 160 bits, Ra and Rb generate the electronic signature to a total of 448 bits, respectively.
[0079] In case a public key certificate is used, using the public key of the public key certificate issue station (CA) 410 which self holds, a user verifies the electronic signature of the public key certificate concerned, after he succeeds in verification of electronic signature, he picks out a public key from a public key certificate, and uses the public key concerned. Therefore, all the users using a public key certificate need to hold the public key of a common public key certificate issue station (CA). In addition, about

the verification approach of electronic signature, since drawing 11 explained, the detail is omitted.

[0080] It verifies whether B of Rb which A has transmitted which received the public key certificate of A, Ra, Rb and Av, and electronic signature A.Sig corresponds with what B generated. Consequently, when in agreement, the electronic signature in the public key certificate of A is verified with the public key of a certificate authority, and the public key of A is taken out. And electronic signature A.Sig is verified using the taken-out public key of A. After succeeding in verification of electronic signature, B attests A as a just thing.

[0081] Next, B generates the random number Bk smaller than Characteristic p. And point Bv=BkxG which doubled the base point G Bk is calculated, electronic signature B.Sig to Rb, Ra, and Bv (X coordinate and Y coordinate) is generated, and A is returned with the public key certificate of B.

[0082] It verifies whether A of Ra which B has transmitted which received the public key certificate of B, Rb, Ra and Bv, and electronic signature B.Sig corresponds with what A generated. Consequently, when in agreement, the electronic signature in the public key certificate of B is verified with the public key of a certificate authority, and the public key of B is taken out. And electronic signature B.Sig is verified using the taken-out public key of B. After succeeding in verification of electronic signature, A attests B as a just thing.

[0083] When both succeed in authentication, B calculates BkxAv (although Bk is a random number, since Av is a point on an elliptic curve, scalar multiple count of the point on an elliptic curve is the need), and A calculates AkxBv, and after using 64 bits of low order of the X coordinate of these points as a session key, it is used for a communication link (when a common key encryptosystem is made into the common key encryptosystem of 64-bit key length). Of course, a session key may be generated from Y coordinate and you may not be 64 bits of low order. In addition, transmit data is not only enciphered with a session key, but electronic signature may be attached in the secret communication after mutual recognition.

[0084] When injustice and an inequality are found on the occasion of verification of electronic signature, or verification of received data, processing is interrupted as that in which mutual recognition failed.

[0085] In such mutual recognition processing, using the generated session key, transmit data is enciphered and data communication is performed mutually.

[0086] (2) If Transaction ID, purchase requested data generation and the (3) purchase requested data transmitting above-mentioned shop server 100, and the mutual recognition between the user machines 200 are successful, the user machine 200 will generate the purchase requested data of contents. The configuration of purchase requested data is shown in drawing 14 (a). Purchase requested data has each data of the content ID as an identifier of the transaction ID which the cipher-processing means of the user machine 200 generates based on a random number as an identifier of the shop ID which is the identifier of the shop server 100 which is the demand place of contents purchase, and contents dealings, and the contents of which a user machine expects purchase further, and the electronic signature of the user machine to these data is added. Furthermore, the public key certificate of a user machine is attached to purchase requested data, and it is sent to the shop server 100. In addition, in the above-

mentioned mutual recognition processing or processing of the before, a public key certificate does not already need to send anew necessarily, when finishing [sending to a shop side].
[0087] (4) The shop server 100 which received the purchase requested data shown in received-data verification drawing 14 (a) from the user machine 200 performs verification processing of received data. The detail of verification processing is explained using drawing 15 . First, the shop server 100 verifies public key certificate Cert_DEV of the user machine in received data (S51). As mentioned above, this is performed as processing (refer to drawing 11) which verifies the signature of the issue office (CA) included in a public key certificate, and is performed with the application of public key:KpCA of an issue office.
[0088] If the alteration of O.K., i.e., a public key certificate, does not have verification and it will be judged (it is Yes at S52), it will progress to S53. When verification is not materialized (it is No at S52), it is judged with those with an alteration by the public key certificate by S57, and processing using the public key certificate is stopped. Public key:KpDEV of a user machine is taken out from a public key certificate, and verification processing (refer to drawing 11) of a user machine signature of the purchase requested data using public key:KpDEV is performed at step S54 S53. If the alteration of O.K., i.e., purchase requested data, does not have verification and it will be judged (it is Yes at S55), it will progress to S56 and will be judged with received data being just contents purchase requested data. When verification is not materialized (it is No at S55), purchase requested data is judged to be those with an alteration, and the processing to the purchase requested data is stopped by S57.
[0089] (5) In encryption contents and the encryption contents key data 1 (shop) transmitting shop server 100, verification of purchase requested data is completed, and if it judges with it being the just contents purchase demand without a data alteration, the shop server 100 will transmit encryption contents and the encryption contents key data 1 (shop) to a user machine. Encryption contents:Kc (content) which each of these is data stored in the contents database 110, and enciphered contents by the contents key, and a contents key: It is encryption contents key data:KpDAS (Kc) which enciphered Kc with the public key of the user machine authentication server (DAS) 300.
[0090] The configuration of the encryption contents key data 1 (shop) is shown in drawing 14 (b). The encryption contents key data 1 (shop) have shop processing No. which the shop server 100 generated with the user machine ID which is the identifier of the user machine 200 which is the demand origin of contents purchase, purchase requested data (data except the user machine public key certificate of drawing 14 (a)), and contents dealings, and encryption contents key data:KpDAS (Kc), and the electronic signature of the shop server 100 to these data is added. Furthermore, the public key certificate of the shop server 100 is attached to the encryption contents key data 1 (shop), and it is sent to the user machine 200. In addition, in the above-mentioned mutual recognition processing or processing of the before, a shop server public key certificate does not already need to send anew necessarily, when finishing [sending to a user machine side].
[0091] (6) From the received-data verification shop server 100 to encryption contents : the user machine 200 which received the encryption contents key data 1 (shop) indicated to be Kc (content) to drawing 14 (b) performs verification processing of the

encryption contents key data 1 (shop). This verification processing is the same processing as the processing flow of drawing 15 explained previously, and the user machine 200 performs verification of the public key certificate of the shop server first received from the shop server 100 using the public key KpCA of an issue office (CA), and performs verification of a shop signature of the encryption contents key data 1 (shop) shown in drawing 14 (b) using the public key KpSHOP of a shop server picked out from the public key certificate next.

[0092] (7) After the mutual recognition user machine 200 receives encryption contents:Kc (content) and the encryption contents key data 1 (shop) from the shop server 100 and finishes verification of the encryption contents key data 1 (shop), the user machine 200 accesses the user machine authentication server 300, and performs mutual recognition processing between the user machine 200 and the user machine authentication server 300. This processing is performed in the same procedure as the above-mentioned shop server 100 and the mutual recognition processing between the user machines 200.

[0093] (8) If it obtains in encryption contents key data (user machine) and an encryption contents key, or ** and the mutual recognition between the demand sending-user machine 200 and the user machine authentication server 300 is materialized, to the user machine authentication server 300, the user machine 200 will be obtained in the encryption contents key data (user machine) containing the encryption contents key KpDAS (Kc) previously received from the shop server 100, and an encryption contents key or **, and will transmit a demand.

[0094] The configuration of encryption contents key data (user machine) is shown in drawing 14 (c). Encryption contents key data (user machine) have encryption contents key data (data except the shop public key certificate of drawing 14 (b)) which obtained in an encryption contents key or ** and were received from user machine authentication server ID which is the identifier of the user machine authentication server 300 which is the demand place of a demand, and the shop server 100, and the electronic signature of the user machine 200 to these data is added. Furthermore, the public key certificate of the shop server 100 and the public key certificate of the user machine 200 are attached to encryption contents key data (user machine), and it is sent to the user machine authentication server 300. In addition, when the user machine authentication server 300 has already held the user machine public key certificate and the shop server public key certificate, it is not necessary to necessarily send anew.

[0095] (9) Obtain the user machine authentication server 300 which obtained from the received-data verification user machine 200 in encryption contents key data (user machine) and an encryption contents key, or **, and received the demand (drawing 14 (c)) in an encryption contents key or **, and it performs verification processing of a demand. This verification processing is the same processing as the processing flow of drawing 15 explained previously. The user machine authentication server 300 Verification of the public key certificate of the user machine first received from the user machine 200 is performed using the public key KpCA of an issue station (CA). Next, verification of the electronic signature of the encryption contents key data (user machine) shown in the purchase requested data and drawing 14 (c) which are shown in drawing 14 (a) is performed using the public key KpDEV of the user machine picked out from the public key certificate. Furthermore, verification of the public key certificate of a

shop server is performed using the public key KpCA of an issue office (CA), and verification of a shop signature of (5) encryption contents key data 1 contained in the encryption contents key data (user machine) shown in drawing 14 (c) using the public key KpSHOP of a shop server picked out from the public key certificate next is performed.

[0096] (10) Obtain in an encryption contents key or ** and set to processing and the user machine authentication server 300. If it judges with it obtaining in the encryption contents key data (user machine) and the encryption contents key, or ** which received from the user machine 200, and verification of a demand being completed, and it obtaining in a just key or **, and being a demand The encryption contents key with which the user machine authentication server 300 is contained in encryption contents key data (user machine), Namely, a contents key : Decode data:KpDAS (Kc) which enciphered Kc with the public key KpDAS of the user machine authentication server (DAS) 300 with the private key KsDAS of the user machine authentication server 300, and the contents key Kc is acquired. further -- the contents key Kc -- public key [of a user machine]: -- encryption contents key: enciphered by KpDEV -- KpDEV (Kc) is generated. That is, it obtains in the key or ** of KpDAS(Kc) ->Kc->KpDEV (Kc), and processing is performed.

[0097] It obtains in the encryption contents key or ** performed by drawing 16 in the user machine authentication server 300, and the flow of processing is shown. First, the user machine authentication server 300 takes out contents key data:KpDAS (Kc) enciphered with the public key KpDAS of the user machine authentication server (DAS) 300 from the encryption contents key data (user machine) received from the user machine 200 (S61). Next, it decodes with the private key KsDAS of the user machine authentication server 300, and the contents key Kc is acquired (S62). Next, the contents key Kc acquired by decode is re-enciphered by public key:KpDEV of a user machine, and encryption contents key:KpDEV (Kc) is generated (S63). Termination of these processings sets up the status of a license management database (refer to drawing 6) for "obtaining in a key or ** and completing."

[0098] (11) In the mutual recognition user machine authentication server 300, if it obtains in the above-mentioned key or above-mentioned ** of an encryption contents key and processing is completed, the user machine authentication server 300 will access the shop server 100, and will perform mutual recognition processing between the user machine authentication server 300 and the shop server 100. This processing is performed in the same procedure as the above-mentioned shop server 100 and the mutual recognition processing between the user machines 200.

[0099] (12) If the mutual recognition between the encryption contents data sending-user machine authentication server 300 and the shop server 100 is materialized, the user machine authentication server 300 will transmit encryption contents key data (DAS) to the shop server 100.

[0100] The configuration of encryption contents key data (DAS) is shown in drawing 17 (d). The shop ID which is the identifier of the shop server 100 whose encryption contents key data (DAS) are the demand place of contents purchase It obtains in encryption contents key data (user machine) (data except the shop of drawing 14 (c), and a user machine public key certificate), and the further above-mentioned key or **. By processing Encryption contents key data which the user machine authentication

server 300 generated: It has KpDEV (Kc) and the electronic signature of the user machine authentication server 300 to these data is added. Furthermore, the user machine authentication server 300 and the public key certificate of the user machine 200 are attached to encryption contents key data (DAS), and it is sent to the shop server 100. In addition, when a shop server is already possession ending, it does not necessarily need to send these public key certificates anew.

[0101] Moreover, when it is the existence accepted to be the independent organization which can trust the user machine authentication server 300 Without considering as the data configuration which contains (8) encryption contents key data (user machine) which the user machine generated as it is, as shown in drawing 17 (d), as shown in drawing 18 (d'), encryption contents key data (DAS) The user machine authentication server 300 extracts each data of the contents key KpDEV (Kc) enciphered with the public key of the user machine ID, Transaction ID, content ID, the shop processing NO, and a user device. A signature is added to these and it is good also as encryption contents key data (DAS). In this case, since verification of (8) encryption contents key data (user machine) becomes unnecessary, the public key certificate to attach is good only with the public key certificate of the user machine authentication server 300.

[0102] (13) The shop server 100 which received encryption contents key data (DAS) (drawing 17 (d)) from the received-data verification user machine authentication server 300 performs verification processing of encryption contents key data (DAS). This verification processing is the same processing as the processing flow of drawing 15 explained previously. The shop server 100 Verification of the public key certificate of the user machine authentication server first received from the user machine authentication server 300 is performed using the public key KpCA of an issue station (CA). Next, verification of the electronic signature of the encryption contents key data (DAS) shown in drawing 17 (d) using the public key KpDAS of the user machine authentication server 300 picked out from the public key certificate is performed. Furthermore, verification of the public key certificate of a user machine is performed using the public key KpCA of an issue office (CA), and verification of a user machine signature of (8) encryption contents key data (user machine) contained in the encryption contents key data (DAS) shown in drawing 17 (d) using the public key KpDEV of the user machine picked out from the public key certificate next is performed. Furthermore, you may make it verify encryption contents data (user machine) again using the self public key KpSHOP.

[0103] In addition, when the shop server 100 receives the encryption contents key data (DAS) which were explained previously and which drawing 18 (d') simplified The shop server 100 performs verification of the public key certificate of a user machine authentication server using the public key KpCA of an issue station (CA). Next, it becomes processing of only performing verification of the electronic signature of the encryption contents key data (DAS) shown in drawing 18 (d') using the public key KpDAS of the user machine authentication server 300 picked out from the public key certificate.

[0104] (14) Mutual recognition and (15) encryption contents key requested data transmission, next the user machine 200 transmit encryption contents key requested data to the shop server 100. In addition, when performing a demand in a different session from a pre- demand in this case, mutual recognition is performed again and

encryption contents key requested data is transmitted to the shop server 100 from the user machine 200 a condition [mutual recognition having been materialized].
[0105] The configuration of encryption contents key requested data is shown in drawing 17 (e). The shop ID which is the identifier of the shop server 100 whose encryption contents key requested data is the demand place of contents purchase The transaction ID which is the identifier of the contents dealings which the user machine 200 generated previously Furthermore, the content ID as an identifier of the contents of which a user machine expects purchase, Furthermore, it has shop processing No. contained in the data (refer to drawing 14 (b)) which the shop generated previously and have been transmitted to the user machine 200 as encryption contents key data 1 (shop), and the electronic signature of the user machine to these data is added. Furthermore, the public key certificate of a user machine is attached to encryption contents key requested data, and it is sent to the shop server 100. In addition, a public key certificate does not necessarily need to send anew, when finishing [the storage to a shop side] already.
[0106] (16) Verification processing and the shop server 100 which received (17) accounting encryption contents key requested data from the user machine perform verification processing of encryption contents key requested data. This is the processing same with having explained using drawing 15 . If data verification ends, the shop server 100 will perform accounting about dealings of contents. Accounting is processing which receives a contents tariff from a user's dealings account. The received contents tariff is distributed to various persons concerned, such as a copyright person of contents, a shop, and a user machine authentication server manager.
[0107] By the time it results in this accounting, since the treatment process is indispensable, the shop server 100 cannot perform accounting by processing only between user machines by obtaining in the key or ** of an encryption contents key by the user machine authentication server 300. Moreover, since decode of an encryption contents key cannot be performed in the user machine 200, use of contents cannot be performed. The contents of contents dealings which the user machine authentication server obtained in all keys or ** in the user machine authentication server license management database explained using drawing 6 , and performed processing are recorded, and the grasp of the contents dealings used as all the candidates for accounting is attained. Therefore, the contents dealings by the shop side independent become impossible, and an unjust contents sale is prevented.
[0108] (18) After the accounting in the encryption contents key data 2 (shop) transmitting shop server 100 is completed, the shop server 100 transmits the encryption contents key data 2 (shop) to the user machine 200.
[0109] The configuration of the encryption contents key data 2 (shop) is shown in drawing 17 (f). The encryption contents key data 2 (shop) have encryption contents key data (DAS) (data except the user machine of drawing 17 (d), and a user machine authentication server public key certificate) received from the user machine ID which is the identifier of the user machine 200 which is the demand origin of an encryption contents key demand, and the user machine authentication server 300, and the electronic signature of the shop server 100 to these data is added. Furthermore, the public key certificate of the shop server 100 and the public key certificate of the user machine authentication server 300 are attached to the encryption contents key data 2 (shop), and it is sent to the user machine 200. In addition, when the user machine 200

has already held the user machine authentication server public key certificate and the shop server public key certificate, it is not necessary to necessarily send anew.
[0110] In addition, when it is the existence accepted to be the independent organization which can trust the user machine authentication server 300 and the encryption contents key data (DAS) which the shop server 100 receives from the user machine authentication server 300 are encryption contents key data (DAS) which were explained previously and which drawing 18 (d') simplified, the shop server 100 sends the encryption contents key data 2 (shop) shown in drawing 18 (f') to a user machine. That is, the public key certificate of the shop server 100 and the public key certificate of the user machine authentication server 300 are attached to the data which added the signature of a shop server to the simplified encryption contents key data (DAS) which are shown in drawing 18 (d'), and it sends to the user machine 200.
[0111] (19) From the received-data verification shop server 100, the user machine 200 which received the encryption contents key data 2 (shop) performs verification processing of the encryption contents key data 2 (shop). This verification processing is the same processing as the processing flow of drawing 15 explained previously, and the user machine 200 performs verification of the public key certificate of the shop server first received from the shop server 100 using the public key KpCA of an issue office (CA), and performs verification of the electronic signature of the encryption contents key data 2 (shop) shown in drawing 17 (f) using the public key KpSHOP of the shop server 100 picked out from the public key certificate next. Furthermore, verification of the public key certificate of the user machine authentication server 300 is performed using the public key KpCA of an issue office (CA), and signature verification of (12) encryption contents key data (DAS) contained in the encryption contents key data 2 (shop) shown in drawing 17 (f) using the public key KpDAS of the user machine authentication server 300 picked out from the public key certificate next is performed. You may make it verify encryption contents data (user machine) further again using the self public key KpDEV.
[0112] (20) The user machine 200 which verified the encryption contents key data 2 (shop) received from the preservation processing shop server 100 Encryption contents key:KpDEV (Kc) enciphered with the self public key KpDEV contained in the encryption contents key data 2 (shop) is decoded using the self private key KsDEV. Furthermore, it enciphers using the preservation key Ksto of a user machine, encryption contents key:Ksto (Kc) is generated, and this is stored in the storage means of the user machine 200. Encryption contents key:Ksto (Kc) is decoded using the preservation key Ksto, using the contents key Kc which took out and took out the contents key Kc, in the utilization time of contents, decode processing of the encryption contents Kc (Content) is performed, and contents (Content) are reproduced and performed to it.
[0113] The acquisition of the contents key Kc and preservation processing flow in the user machine 200 are shown in drawing 19 . First, the user machine 200 takes out encryption contents key:KpDEV (Kc) enciphered with the self public key KpDEV from the encryption contents key data 2 (shop) received from the shop server 100 (S71), decodes taken-out encryption contents key:KpDEV (Kc) using the self private key KsDEV, and takes out the contents key Kc (S72). Furthermore, encryption processing of the contents key Kc is performed using the preservation key Ksto of a user machine, encryption contents key:Ksto (Kc) is generated, and this is stored in the storage means (internal memory) of the user machine 200 (S73).

[0114] By the above processing, a user machine can acquire the contents key Kc of the encryption contents Kc (Content) and these encryption contents, and can use contents. clear from above-mentioned explanation -- as -- the user machine 200 -- setting -- contents -- until it results in an available condition -- **** -- it obtains in the key or ** of an encryption contents key in the user machine authentication server 300, and a treatment process is indispensable. Therefore, to the user machine 200, the shop server 100 cannot sell contents to the user machine authentication server 300 secretly, and cannot make contents an available condition in a user machine. A user machine authentication server in the user machine authentication server license management database explained using drawing 6 All keys, **, or the contents of contents dealings that obtained and performed processing is recorded. Management of dealings of all shops is made and the charged contents dealings are grasped. It becomes possible to distribute correctly the contents tariff received in the accounting of a shop to various persons concerned, such as a copyright person of contents, a shop, and a user machine authentication server manager.

[0115] (Status transition in each device) The shop server 100 and the user machine 200 which are shown in drawing 1 , and the user authentication server (DAS) 300 opt for the next processing in a series of processings which relate to contents dealings, respectively according to the status which shows a processing state. The status is managed for every contents dealings in the purchase management database of a shop server shown in drawing 3 , the license management database of the user machine authentication server of drawing 6 , and the purchase management database of the user machine of drawing 8 .

[0116] First, status transition of the shop server 100 is explained using drawing 20 . Processing is started because a shop server receives the contents purchase requested data from the user machine 200 (it corresponds to processing (3) of drawing 1). The shop server 100 sets the status as "the completion of purchase reception", when the received data from the user machine 200 are verified and it succeeds in verification, and when judgment that it is a just purchase demand is not made by data verification, processing is stopped, or the same processing and here the after treatment repeated purchase reception processing the number of predetermined times is stopped, and it carries out the status as "purchase reception failure." Only when the status is "the completion of purchase reception", it progresses to degree step.

[0117] If the status changes to "the completion of purchase reception" next, the shop server 100 will consider the status as "the completion of key 1 distribution" by transmitting the encryption contents key data 1 (shop) to the user machine 200 (it corresponding to processing (5) of drawing 1), and receiving the reception response (response) from a user machine. When transmission of the key data 1 is not successful, processing is stopped, or after repeating transmitting processing of the key data 1 the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key 1 distribution failure." Only when the status is "the completion of key 1 distribution", it progresses to degree step.

[0118] When the status changes to "the completion of key 1 distribution" next, the shop server 100 receives encryption contents key data (DAS) from the user machine authentication server 300 (it corresponds to processing (12) of drawing 1), and performs data verification. When it succeeds in verification, the status is set as "the

completion of key reception", when judgment that it is just encryption contents key data (DAS) is not made by data verification, processing is stopped, or after repeating key reception the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key reception failure." Only when the status is "the completion of key reception", it progresses to degree step.
[0119] When the status changes to "the completion of key reception" next, the shop server 100 receives encryption contents key Request-to-Send data from the user machine 200 (it corresponds to processing (15) of drawing 1), and performs data verification. When it succeeds in verification, the status is set as "the completion of encryption contents key Request-to-Send reception", when judgment that it is just key Request-to-Send data is not made by data verification, processing is stopped, or after repeating the reception of encryption contents key Request-to-Send data the number of predetermined times, processing is stopped by the same processing and here, and the status is carried out as "encryption contents key Request-to-Send reception failure." Only when the status is "the completion of encryption contents key Request-to-Send reception", it progresses to degree step.
[0120] When the status changes to "the completion of encryption contents key Request-to-Send reception" next, the shop server 100 performs accounting (it corresponds to processing (17) of drawing 1). When accounting was completed, the status is set as "the completion of accounting" and accounting is not completed (for example, when contents tariff pulling down from the designated account of a user machine is not completed), subsequent processings are not performed, but stop processing, or after they repeat accounting the number of predetermined times, they stop processing by the same processing and here, and consider the status as "accounting failure." Only when the status is "the completion of accounting", it progresses to degree step.
[0121] When the status changes to "the completion of accounting" next, the shop server 100 performs encryption contents key data 2 (shop) transmitting processing (it corresponds to processing (18) of drawing 1) to a user machine. When encryption contents key data 2 (shop) transmitting processing is completed, the receiving response from a user machine was received, the status is set as "the completion of key 2 distribution" and key data 2 (shop) transmitting processing is not completed, the status is considered as "key 2 distribution failure." Only when the status is "the completion of key 2 distribution", it becomes processing termination degree step and here, and when the status is "key 2 distribution failure", subsequent processings are not performed, stop processing, or repeat key data 2 (shop) transmitting processing the number of predetermined times the same processing and here. The shop server 100 performs such a state transition for every contents dealings.
[0122] Next, status transition of the user machine 200 is explained using drawing 21 . Processing is started because the user machine 200 transmits contents purchase requested data to the shop server 100 first (it corresponds to processing (3) of drawing 1). Processing is stopped, or after repeating purchase demand transmitting processing the number of predetermined times, the same processing and here processing stops, and a user machine 200 carries out the status as "purchase demand transmitting failure", when the status is set up to "the completion of purchase demand transmitting" and the response of the completion of reception from the shop server 100 cannot be received, if the response of the completion of reception of contents purchase requested

data to the shop server 100 is received. Only when the status is "the completion of purchase demand transmitting", it progresses to degree step.
[0123] If the status changes to "the completion of purchase demand transmitting" next, from the shop server 100, the user machine 200 will receive the encryption contents key data 1 (shop) (it corresponds to processing (5) of drawing 1), and will verify received data. When it succeeds in verification of the encryption contents key data from the shop server 100, the status is set as "the completion of key 1 reception", when judgment that it is just encryption contents key data is not made by data verification, processing is stopped, or after repeating key 1 reception the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key 1 reception failure." Only when the status is "the completion of key 1 reception", it progresses to degree step.
[0124] When the status changes to "the completion of key 1 reception" next, to the user machine authentication server 300, the user machine 200 transmits encryption contents key data (user machine) (it corresponds to processing (8) of drawing 1), and receives a data receiving response. When a data receiving response is received, the status is set as "the completion of key transmitting", when not receiving a data receiving response, processing is stopped, or after repeating key transmitting processing the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key transmitting failure." Only when the status is "the completion of key transmitting", it progresses to degree step.
[0125] When the status changes to "the completion of key transmitting" next, to the shop server 100, the user machine 200 transmits an encryption contents key Request to Send (it corresponds to processing (15) of drawing 1), and receives a data receiving response. When a data receiving response is received, the status is set as "the completion of encryption contents key Request-to-Send transmitting", when not receiving a data receiving response, after stopping processing or repeating encryption contents key Request-to-Send transmitting processing the number of predetermined times the same processing and here, processing is stopped and the status is carried out as "encryption contents key Request-to-Send transmitting failure." Only when the status is "the completion of encryption contents key Request-to-Send transmitting", it progresses to degree step.
[0126] When the status changes to "the completion of encryption contents key Request-to-Send transmitting" next, from the shop server 100, the user machine 200 receives the encryption contents key data 2 (shop) (it corresponds to processing (18) of drawing 1), and performs data verification. When it succeeds in data verification, the status is set as "the completion of key 2 reception", when it does not succeed in data verification, processing is stopped, or after repeating key data 2 (shop) reception the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key 2 reception failure." It becomes processing termination when the status is "the completion of key 2 reception." The user machine 200 performs such a state transition for every contents dealings.
[0127] Next, status transition of the user machine authentication server 300 is explained using drawing 22 . Processing is started because the user machine authentication server 300 receives the encryption contents key data (user machine) from the user machine 200 (it corresponds to processing (8) of drawing 1). When the user machine

authentication server 300 verifies the received data from the user machine 200 and it succeeds in verification When the status is set as "the completion of key reception" and judgment that it is just data is not made by data verification Processing is stopped, or after repeating the reception of encryption contents key data (user machine) the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key reception failure." Only when the status is "the completion of key reception", it progresses to degree step.

[0128] If the status changes to "the completion of key reception" next, the user machine authentication server 300 will presuppose the status "is completed [it obtains in a key or ** and]", when obtain, it performs processing (it corresponds to processing (10) of drawing 1), it obtains in a key or ** and processing is completed, a contents key, **, or. Since it does not assume a key, **, or that obtaining goes wrong, status transition of "obtaining in a key or ** and completing" exists here.

[0129] When the status changes "to obtain in a key or ** and complete" next, the user machine authentication server 300 transmits encryption contents key data (DAS) to the shop server 100 (it corresponds to processing (12) of drawing 1), and receives the data reception response from the shop server 100. When a data reception response is received, the status is set as "the completion of key transmitting", when reception of a data reception response is not made, after stopping processing or repeating transmitting processing of encryption contents key data (DAS) the number of predetermined times the same processing and here, processing is stopped and the status is carried out as "key transmitting failure." It becomes processing termination when the status is "the completion of key transmitting." The user machine authentication server 300 performs such a state transition for every contents dealings.

[0130] (Contents purchase processing flow) Next, the data transmitting and receiving processing performed with the contents purchase demand to a shop server between the shop server 100, the user machine 200, and the user machine authentication server 300 from a user machine is explained according to a flow. A processing flow is divided and explained to the following A, B, C, and D.

[0131] A. Processing between a shop server and a user machine (processing of (1) - (6) shown in drawing 1)

Transmission of the key 1 (shop) to the user machine 200 from the contents purchase demand to the shop server 100 from the user machine 200, and the mutual recognition of the shop server 100 - the user machine 200 - the shop server 100.

B. Processing between a user machine authentication server and a user machine (processing of (7) - (9) shown in drawing 1)

Received-data verification in the mutual recognition [of the user machine 200 and the user machine authentication server 300] encryption contents key data transmission - user machine authentication server 300.

C. Processing between a user machine authentication server and a shop server (processing of (11) - (13) shown in drawing 1)

Received-data verification in a mutual recognition [between the user machine authentication server 300 and the shop server 100] encryption contents key data (DAS) transmission - shop server.

D. Processing between a shop server and a user machine (processing of (14) - (19) shown in drawing 1)

Received-data verification in the transmission - user machine 200 of the key 2 (shop) to the user machine 200 from the encryption contents key requested data transmission - shop server 100 to the shop server 100 from the user machine 200, and the mutual recognition of the shop server 100 - the user machine 200.

[0132] First, the processing between A. shop server and a user machine (processing of (1) - (6) shown in drawing 1) is explained using drawing 23 and drawing 24 .

[0133] In drawing 23 and drawing 24 , left-hand side shows processing of a shop server, and right-hand side shows processing of a user machine. In addition, in all flows, the processing step No of S20xx and a user machine authentication server is shown [the processing step No of a shop server] for the processing step No of S10xx and a user machine as S30xx.

[0134] First, as shown in drawing 23 , mutual recognition is performed between a shop server and a user machine at the time of processing initiation (S1001, S2001). Mutual recognition processing is performed as processing explained using drawing 12 or drawing 13 . Using the session key generated in mutual recognition processing, transmit data is enciphered if needed and data communication is performed. If mutual recognition is materialized, a shop server will make new shop processing NO a new processing entry, and will add it to a purchase management database (refer to drawing 3) (S1003).

[0135] On the other hand, if mutual recognition is materialized, a user machine generates the transaction ID applied in these contents dealings based on a random number, will make the new transaction ID a new entry, and will add it to a purchase database (refer to drawing 8) (S2003). Furthermore, a user machine performs transmission of the contents purchase requested data to a shop server (S2004), i.e., transmission of (3) purchase requested data shown in drawing 14 (a).

[0136] A shop server receives the contents purchase requested data from a user machine (S1004), and performs verification of received data (S1005). Data verification is processing according to the processing flow of drawing 11 explained previously. If being just data without an alteration of data is admited by verification of received data, the response of Reception O.K. will be transmitted to a user machine (S1008), and the status of a purchase management database will be set as "the completion of purchase reception" by it (S1010). If data are accepted to be unjust data with an alteration by verification of received data, the response of Reception NG will be transmitted to a user machine (S1007), and the status of a purchase management database will be set as "purchase reception failure" by it (S1009).

[0137] A user machine will set the status of a purchase management database as "the completion of purchase demand transmitting", if the response of the reception O.K. from a shop server is received (it is Yes at S2005 and S2006), and if the receiving NG response from a shop server is received (it is No at S2005 and S2006), it will set the status of a purchase management database as "purchase demand transmitting failure."

[0138] In a shop server, in the status of a purchase management database, generate the encryption contents key data 1 (shop) (refer to drawing 14 (b)) after a setup (S1010) to "the completion of purchase reception" (S1011), and a user machine is received. Contents key: It is Kc, transmit enciphered encryption contents:Kc (Content) (S1012), and transmit further the encryption contents key data 1 (shop) shown in drawing 14 (b) (S1013).

[0139] Encryption contents as which the user machine enciphered the status of a purchase management database from the shop server by contents key:Kc after the setup (S2007) to "the completion of purchase demand transmitting": Receive Kc (Content) (S2009) and receive the encryption contents key data 1 (shop) (drawing 14 (b)) from a shop server further (S2010).
[0140] A user machine performs verification processing (refer to drawing 11) of the data received at steps S2009 and S2010 (S2021), if being just data without an alteration of data is admited by verification of received data, will transmit the response of Reception O.K. to a shop server (S2023), and will set the status of a purchase management database as "the completion of key 1 reception" by it (S2025). If data are accepted to be unjust data with an alteration by verification of received data, after transmitting the response of Reception NG to a shop server (S2024) and setting the status of a purchase management database as "key 1 reception failure" by it (S2026), connection with a shop server is cut (S2027).
[0141] A shop server receives the response from a user machine (S1021), and when a response is O.K., it sets the status of a purchase management database as "a key 1 distribution success" (S1024). When a response is NG, after setting the status of a purchase management database as "key 1 distribution failure" (S1023), connection with a user machine is cut (S1025).
[0142] In addition, in mutual recognition failure of steps S1002 and S2002, in a setup of a setup of "purchase reception failure" of the status of S1009, and "purchase demand transmitting failure" of the status of S2008, processing is all stopped, it performs processing which cuts connection, and considers it as processing termination.
[0143] Next, the processing between B. user machine authentication server and a user machine (processing of (7) - (9) shown in drawing 1) is explained according to the flow of drawing 25 .
[0144] First, mutual recognition is performed between a user machine authentication server and a user machine (S3001, S2031). Mutual recognition processing is performed as processing explained using drawing 12 or drawing 13 . Using the session key generated in mutual recognition processing, transmit data is enciphered if needed and data communication is performed. If mutual recognition is materialized, a user machine authentication server will add first-time-user machine authentication server processing NO to a license management database (refer to drawing 6) as a new processing entry (S3003).
[0145] On the other hand, if mutual recognition is materialized, a user machine will generate encryption contents key data (user machine) (refer to drawing 14 (c)) (S2033), and will transmit them to a user machine authentication server (S2034).
[0146] A user machine authentication server receives the encryption contents key data (user machine) from a user machine (S3004), and performs verification (S3005) of received data. Data verification is processing according to the processing flow of drawing 11 explained previously. If being just data without an alteration of data is admited by verification of received data, the response of Reception O.K. will be transmitted to a user machine (S3008), and the status of a license management database will be set as "the completion of key reception" by it (S3010). If data are accepted to be unjust data with an alteration by verification of received data, the response of Reception NG will be transmitted to a user machine (S3007), and

connection with a user machine will be cut for the status of a license management database after a setup (S3009) to "key reception failure" by it (S3011).
[0147] If the response of the reception O.K. from a user machine authentication server is received (it is Yes at S2035 and S2036), a user machine If the status of a purchase management database is set as "the completion of key transmitting" (S2037) and the receiving NG response from a user machine authentication server is received (it is No at S2035 and S2036) After setting the status of a purchase management database as "key transmitting failure" (S2038), connection with a user machine authentication server is cut (S2039).
[0148] In addition, in mutual recognition failure of steps S3002 and S2032, processing is stopped, it performs processing which cuts connection, and considers it as processing termination.
[0149] Next, the processing between C. user machine authentication server and a shop server (processing of (11) - (13) shown in drawing 1) is explained according to the flow of drawing 26 .
[0150] First, mutual recognition is performed between a user machine authentication server and a shop server (S3021, S1031). Mutual recognition processing is performed as processing explained using drawing 12 or drawing 13 . Using the session key generated in mutual recognition processing, transmit data is enciphered if needed and data communication is performed. If mutual recognition is materialized, a user machine authentication server will generate encryption contents key data (DAS) (refer to drawing 17 (d)) (S3023), and will transmit to a shop server (S3024).
[0151] On the other hand, a shop server receives encryption contents key data (DAS) (refer to drawing 17 (d)) from a user machine authentication server after formation of mutual recognition (S1033), and performs verification (S1034) of received data. Data verification is processing according to the processing flow of drawing 11 explained previously. If being just data without an alteration of data is admited by verification of received data, the response of Reception O.K. will be transmitted to a user machine authentication server (S1036), and the status of a purchase management database will be set as "the completion of key reception" by it (S1038). If data are accepted to be unjust data with an alteration by verification of received data, the response of Reception NG will be transmitted to a user machine authentication server (S1037), and connection with a user machine authentication server will be cut for the status of a purchase management database after a setup (S1039) to "key reception failure" by it (S1040).
[0152] If the response of the reception O.K. from a shop server is received (it is Yes at S3025 and S3026), a user machine authentication server If the status of a license management database is set as "the completion of key transmitting" (S3028) and the receiving NG response from a shop server is received (it is No at S3025 and S3026) After setting the status of a license management database as "key transmitting failure" (S3027), connection with a user machine authentication server is cut (S3029).
[0153] In addition, in mutual recognition failure of steps S3022 and S1032, processing is stopped, it performs processing which cuts connection, and considers it as processing termination.
[0154] Next, the processing between D. shop server and a user machine (processing of (14) - (19) shown in drawing 1) is explained using drawing 27 and drawing 28 .

[0155] First, mutual recognition is performed between a shop server and a user machine at the time of processing initiation (S1051, S2051). Mutual recognition processing is performed as processing explained using drawing 12 or drawing 13 . Using the session key generated in mutual recognition processing, transmit data is enciphered if needed and data communication is performed. If mutual recognition is materialized, a user machine will generate encryption contents key Request-to-Send data (refer to drawing 17 (e)) (S2053), and will transmit them to a shop server (S2054).
[0156] A shop server receives the encryption contents key Request-to-Send data from a user machine (S1054), and performs verification of received data (S1055). Data verification is processing according to the processing flow of drawing 11 explained previously. If being just data without an alteration of data is admited by verification of received data, the response of Reception O.K. will be transmitted to a user machine (S1058), and the status of a purchase management database will be set as "the completion of encryption contents key Request-to-Send reception" by it (S1060). If data are accepted to be unjust data with an alteration by verification of received data, the response of Reception NG will be transmitted to a user machine (S1057), and the status of a purchase management database will be set as "encryption contents key Request-to-Send reception failure" by it (S1059).
[0157] A user machine will set the status of a purchase management database as "the completion of encryption contents key Request-to-Send transmitting", if the response of the reception O.K. from a shop server is received (it is Yes at S2055 and S2056) (S2057), and if the receiving NG response from a shop server is received (it is No at S2055 and S2056), it will set the status of a purchase management database as "encryption contents key Request-to-Send transmitting failure" (S2058).
[0158] In a shop server, the encryption contents key data 2 (shop) which generate the encryption contents key data 2 (shop) (refer to drawing 17 (f)) after a setup (S1060) to "the completion of encryption contents key Request-to-Send reception" (S1061), and show the status of a purchase management database to drawing 17 (f) to a user machine are transmitted (S1062).
[0159] A user machine receives the encryption contents key data 2 (shop) (drawing 17 (f)) for the status of a purchase management database from a shop server after a setup (S2057) to "the completion of encryption contents key Request-to-Send transmitting" (S2059).
[0160] A user machine performs verification processing (refer to drawing 11) of the data received at step S2059 (S2071), if being just data without an alteration of data is admited by verification of received data, will transmit the response of Reception O.K. to a shop server (S2073), and will set the status of a purchase management database as "the completion of key 2 reception" by it (S2075). If data are accepted to be unjust data with an alteration by verification of received data, after transmitting the response of Reception NG to a shop server (S2074) and setting the status of a purchase management database as "key 2 reception failure" by it (S2076), connection with a shop server is cut (S2077).
[0161] A shop server receives the response from a user machine (S1071), and when a response is O.K., it sets the status of a purchase management database as "a key 2 distribution success" (S1074). When a response is NG, after setting the status of a

purchase management database as "key 2 distribution failure" (S1073), connection with a user machine is cut (S1075).
[0162] In addition, in mutual recognition failure of steps S1052 and S2052, processing is stopped, it performs processing which cuts connection, and considers it as processing termination.
[0163] [the modification of a basic contents distribution model 1] -- although the configuration of contents purchase processing and procedure have explained so far based on the configuration of the basic contents distribution model 1 shown in drawing 1 , if it is a configuration with the policy considered as the configuration which a contents key rechips in a user machine authentication server fundamentally, and performs processing, it is realizable not only in the configuration shown in drawing 1 but various modes Hereafter, various modifications are explained.
[0164] The configuration shown in drawing 29 is a configuration of having separated the function of a shop server and having prepared the shop server and the distribution server. Although the shop server 100 receives the contents purchase demand from the user machine 200, the distribution server 400 performs contents distribution to the user machine 200. In this example, although mutual recognition processing is omitted between each entity, mutual recognition processing may be performed like the basic contents distribution model 1.
[0165] After the shop server 100 receives the purchase requested data from the user machine 200, verifies data (processing of drawing 29 (3)) and checks the justification of requested data, it performs transmission of a contents distribution demand to the distribution server 400 (processing of drawing 29 (4)). The distribution server 400 transmits the encryption contents and encryption contents key data (distribution server) which were picked out from the contents database 410, when the contents distribution requested data from the shop server 100 is verified and the justification of data is checked (processing of drawing 29 (6)). Encryption contents key data (distribution server) are the contents key Kc which corresponded to the encryption contents key data 1 (shop) of the above-mentioned example, and was enciphered with the public key KpDAS of a user machine authentication server, i.e., the data containing KpDAS (Kc).
[0166] The processing after the user machine 200 received encryption contents and encryption contents key data (distribution server) from the distribution server 400 becomes being the same as that of the example based on the configuration shown in previous drawing 1 .
[0167] In this configuration, the shop server 100 receives the contents demand from a user machine, is reapplied from the function and user machine authentication server which verify the justification, receives a settled encryption contents key, mainly performs distribution to a user machine, and does not perform management of the contents itself, and distribution. It is a mode suitable for the configuration which transmits a contents distribution demand to the distribution server to which one shop server answers a contents demand from a user machine to two or more distribution servers used as various contents administration, such as a music content distribution server which follows, for example, manages music data, and a game contents distribution server which manages game contents, and a shop server manages demand contents according to a demand. Moreover, since for example, a user machine and a shop server are two-way communication by having made it this configuration, the Internet is

used, but from a distribution server, to a user machine, since it is one-way communication, there is a merit which can use high-speed satellite communication.
[0168] Drawing 30 is the configuration of having separated the function of a shop server like drawing 29 , and having prepared the shop server and the distribution server, and although the shop server 100 receives the contents purchase demand from the user machine 200, the distribution server 400 performs contents distribution to the user machine 200. A different point from the configuration of drawing 29 is a point considered as the configuration to which a contents distribution demand is not transmitted from the shop server 100 to the distribution server 400, but the user machine authentication server 300 transmits a contents distribution demand to the distribution server 400.
[0169] After the shop server 100 receives the purchase requested data from the user machine 200, verifies data (processing of drawing 30 (3)) and checks the justification of requested data, it performs transmission of a contents distribution demand to the user machine authentication server 300 (processing of drawing 30 (4)). Then, after the user machine authentication server 300 verifies data (processing of drawing 30 (5)) and checks the justification of requested data, it performs transmission of a contents distribution demand to the distribution server 400 (processing of drawing 30 (6)). The distribution server 400 transmits the encryption contents and encryption contents key data (distribution server) which were picked out from the contents database 410 to the user machine 200, when the contents distribution requested data from the user machine authentication server 300 is verified and justification is checked (processing of drawing 30 (8)). Encryption contents key data (distribution server) are the contents key Kc which corresponded to the encryption contents key data 1 (shop) of the above-mentioned example, and was enciphered with the public key KpDAS of a user machine authentication server, i.e., the data containing KpDAS (Kc).
[0170] The processing after the user machine 200 received encryption contents and encryption contents key data (distribution server) from the distribution server 400 becomes being the same as that of the example based on the configuration shown in previous drawing 1 .
[0171] In this configuration, when the key from the user machine 200 reapplies the user machine authentication server 300 and it has a contents purchase demand to the shop server 100 before a demand, it becomes possible [acquiring and managing the user machine information which is a contents purchase demand subject]. Therefore, the key from the user machine 200 rechips, and collating processing of whether to be a registered contents purchase demand user machine is already attained at the time of demand receipt.
[0172] [1.3. Basic contents distribution model 2], next a different basic contents distribution model 2 from the basic contents distribution model 1 using drawing 31 are explained. In the basic contents distribution model 2, data transmission and reception are not performed between the user machine 200 and the user machine authentication server 300. Each processing (1) - (19) shown in drawing 31 is explained focusing on difference with the basic contents distribution model 1. In addition, although this example has described what performed mutual recognition processing ((1), (7), (13)) in the communication link between entities, you may omit if needed.
[0173] (1) The user machine 200 which is going to purchase mutual recognition contents from the shop server 100 performs mutual recognition processing between the

shop servers 100. Mutual recognition processing is the processing explained using drawing 12 or drawing 13 . In mutual recognition processing, using the generated session key, transmit data is enciphered if needed and data communication is performed.

[0174] (2) If the mutual recognition between Transaction ID, purchase requested data generation, and (3) purchase requested data transmitting shop server 100 and the user machine 200 is successful, the user machine 200 will generate the purchase requested data of contents. The configuration of purchase requested data is shown in drawing 32 (g). Purchase requested data has each data of the content ID as an identifier of the transaction ID which the cipher-processing means of the user machine 200 generates based on a random number as an identifier of the shop ID which is the identifier of the shop server 100 which is the demand place of contents purchase, and contents dealings, and the contents of which a user machine expects purchase further, and the electronic signature of the user machine to these data is added. Furthermore, the public key certificate of a user machine is attached to purchase requested data, and it is sent to the shop server 100. In addition, in the above-mentioned mutual recognition processing or processing of the before, a public key certificate does not already need to send anew necessarily, when finishing [sending to a shop side].

[0175] (4) The shop server 100 which received the purchase requested data shown in received-data verification drawing 32 (g) from the user machine 200 performs verification processing of received data. The detail of verification processing is as having explained using drawing 15 previously.

[0176] (5) In encryption contents and the purchase reception data transmitting shop server 100, verification of purchase requested data is completed, and if it judges with it being the just contents purchase demand without a data alteration, the shop server 100 will transmit encryption contents and purchase reception data to a user machine. Encryption contents as which these enciphered contents by the contents key: It is data of only indicating it to be Kc (content) to have received the purchase demand, and is data which do not contain encryption contents key data:KpDAS (Kc) which enciphered previous contents key:Kc with the public key of the user machine authentication server (DAS) 300.

[0177] The configuration of purchase reception data is shown in drawing 32 (h). Purchase reception data have shop processing No. which the shop server 100 generated with the user machine ID which is the identifier of the user machine 200 which is the demand origin of contents purchase, purchase requested data (data except the user machine public key certificate of drawing 32 (g)), and contents dealings, and the electronic signature of the shop server 100 to these data is added. Furthermore, the public key certificate of the shop server 100 is attached to purchase reception data, and it is sent to the user machine 200. In addition, in the above-mentioned mutual recognition processing or processing of the before, a shop server public key certificate does not already need to send anew necessarily, when finishing [sending to a user machine side].

[0178] (6) From the received-data verification shop server 100 to encryption contents : the user machine 200 which received the purchase reception data indicated to be Kc (content) to drawing 32 (h) performs verification processing of purchase reception data. This verification processing is the same processing as the processing flow of drawing

15 explained previously, and the user machine 200 performs verification of the public key certificate of the shop server first received from the shop server 100 using the public key KpCA of an issue office (CA), and performs verification of a shop signature of the purchase reception data shown in drawing 32 (h) using the public key KpSHOP of a shop server picked out from the public key certificate next.

[0179] (7) mutual recognition (8) encryption contents key data -- 1 (shop) ****, next, the shop server 100 accesses the user machine authentication server 300, and performs mutual recognition processing between the shop server 100 and the user machine authentication server 300. If mutual recognition is materialized, the shop server 100 will transmit the encryption contents key data 1 (shop) to the user machine authentication server 300.

[0180] The configuration of the encryption contents key data 1 (shop) is shown in drawing 32 (i). The encryption contents key data 1 (shop) have the purchase requested data (data except the user machine public key certificate of drawing 32 (g)) and shop processing No. which obtained in an encryption contents key or ** and were received from user machine authentication server ID which is the identifier of the user machine authentication server 300 which is the demand place of a demand, and the user machine 200, and the electronic signature of the shop server 100 to these data is added. Furthermore, the public key certificate of the shop server 100 and the public key certificate of the user machine 200 are attached to the encryption contents key data 1 (shop), and it is sent to the user machine authentication server 300. In addition, when the user machine authentication server 300 has already held the user machine public key certificate and the shop server public key certificate, it is not necessary to necessarily send anew.

[0181] (9) The user machine authentication server 300 which received the encryption contents key data 1 (shop) (drawing 32 (i)) from the received-data verification shop server 100 performs verification processing of received data. This verification processing is the same processing as the processing flow of drawing 15 explained previously, and the user machine authentication server 300 performs verification of the public key certificate of the shop server first received from the shop server 100 using the public key KpCA of an issue office (CA), and performs verification of the electronic signature of the encryption contents key data 1 (shop) shown in drawing 32 (i) using the public key KpSHOP of a shop server picked out from the public key certificate next. Furthermore, verification of the public key certificate of a user machine is performed using the public key KpCA of an issue office (CA), and verification of a user machine signature of (3) purchase requested data contained in the encryption contents key data 1 (shop) shown in drawing 32 (i) using the public key KpDEV of the user machine picked out from the public key certificate next is performed.

[0182] (10) Obtain in an encryption contents key or ** and set to the processing user machine authentication server 300. When it judges with the verification of the encryption contents key data 1 (shop) which received from the shop server 100 being completed, and it being just data, the user machine authentication server 300 The encryption contents key contained in the encryption contents key data 1 (shop), Namely, a contents key : Decode data:KpDAS (Kc) which enciphered Kc with the public key KpDAS of the user machine authentication server (DAS) 300 with the private key KsDAS of the user machine authentication server 300, and the contents key Kc is

acquired. further -- the contents key Kc -- public key [of a user machine]: -- encryption contents key: enciphered by KpDEV -- KpDEV (Kc) is generated. That is, it obtains in the key or ** of KpDAS(Kc) ->Kc->KpDEV (Kc), and processing is performed. This processing is processing according to the flow shown in drawing 16 explained previously.

[0183] (11) Encryption contents data transmission, next the user machine authentication server 300 transmit encryption contents key data (DAS) to the shop server 100.

[0184] The configuration of encryption contents key data (DAS) is shown in drawing 33 (j). The shop ID which is the identifier of the shop server 100 whose encryption contents key data (DAS) are the demand place of contents purchase It obtains in the encryption contents key data 1 (shop) (data except the shop of drawing 32 (i), and a user machine public key certificate), and the further above-mentioned key or **. By processing Encryption contents key data which the user machine authentication server 300 generated: It has KpDEV (Kc) and the electronic signature of the user machine authentication server 300 to these data is added. Furthermore, the user machine authentication server 300 and the public key certificate of the user machine 200 are attached to encryption contents key data (DAS), and it is sent to the shop server 100. In addition, when a shop server is already possession ending, it does not necessarily need to send these public key certificates anew.

[0185] Moreover, when it is the existence accepted to be the independent organization which can trust the user machine authentication server 300 Without considering as the data configuration which contains (8) encryption contents key data 1 (shop) as shown in drawing 33 (j) as it is, as shown in drawing 34 (j'), encryption contents key data (DAS) The user machine authentication server 300 extracts each data of the contents key KpDEV (Kc) enciphered with the public key of Shop ID, the user machine ID, Transaction ID, content ID, the shop processing NO, and a user device. A signature is added to these and it is good also as encryption contents key data (DAS). The public key certificate to attach is a public key certificate of the user machine authentication server 300.

[0186] (12) The shop server 100 which received encryption contents key data (DAS) (drawing 33 (j)) from the received-data verification user machine authentication server 300 performs verification processing of encryption contents key data (DAS). This verification processing is the same processing as the processing flow of drawing 15 explained previously. The shop server 100 Verification of the public key certificate of the user machine authentication server first received from the user machine authentication server 300 is performed using the public key KpCA of an issue station (CA). Next, verification of the electronic signature of the encryption contents key data (DAS) shown in drawing 33 (j) using the public key KpDAS of the user machine authentication server 300 picked out from the public key certificate is performed. In addition, same verification is performed also when the shop server 100 receives the encryption contents key data (DAS) which were explained previously and which drawing 34 (j') simplified. Furthermore, you may make it verify the encryption contents key 1 (shop 1) in the encryption contents data (DAS) of drawing 33 (j) if needed.

[0187] (13) Mutual recognition and (14) encryption contents key requested data transmission, next the user machine 200 transmit encryption contents key requested data to a shop server. In addition, when performing a demand in a different session

from a pre- demand in this case, mutual recognition is performed again and encryption contents key requested data is transmitted to the shop server 100 from the user machine 200 a condition [mutual recognition having been materialized].
[0188] (15) Verification processing and the shop server 100 which received (16) accounting encryption contents key requested data from the user machine perform verification processing of encryption contents key requested data. This is the processing same with having explained using drawing 15 . If data verification ends, the shop server 100 will perform accounting about dealings of contents. Accounting is processing which receives a contents tariff from a user's dealings account. The received contents tariff is distributed to various persons concerned, such as a copyright person of contents, a shop, and a user machine authentication server manager.
[0189] Like the basic model 1 mentioned above, by the time it results in this accounting, since the treatment process is indispensable, the shop server 100 cannot perform accounting by processing only between user machines by obtaining in the key or ** of an encryption contents key by the user machine authentication server 300. Moreover, since decode of an encryption contents key cannot be performed in the user machine 200, use of contents cannot be performed. The contents of contents dealings which the user machine authentication server obtained in all keys or ** in the user machine authentication server license management database explained using drawing 6 , and performed processing are recorded, and the grasp of the contents dealings used as all the candidates for accounting is attained. Therefore, the contents dealings by the shop side independent become impossible, and an unjust contents sale is prevented.
[0190] (17) After the accounting in the encryption contents key data 2 (shop) transmitting shop server 100 is completed, the shop server 100 transmits the encryption contents key data 2 (shop) to the user machine 200.
[0191] The configuration of the encryption contents key data 2 (shop) is shown in drawing 33 (k). The encryption contents key data 2 (shop) have encryption contents key data (DAS) (data except the user machine authentication server public key certificate of drawing 33 (j)) received from the user machine ID which is the identifier of the user machine 200 which is the demand origin of an encryption contents key demand, and the user machine authentication server 300, and the electronic signature of the shop server 100 to these data is added. Furthermore, the public key certificate of the shop server 100 and the public key certificate of the user machine authentication server 300 are attached to the encryption contents key data 2 (shop), and it is sent to the user machine 200. In addition, when the user machine 200 has already held the user machine authentication server public key certificate and the shop server public key certificate, it is not necessary to necessarily send anew.
[0192] In addition, when it is the existence accepted to be the independent organization which can trust the user machine authentication server 300 and the encryption contents key data (DAS) which the shop server 100 receives from the user machine authentication server 300 are encryption contents key data (DAS) which were explained previously and which drawing 34 (j') simplified, the shop server 100 sends the encryption contents key data 2 (shop) shown in drawing 34 (k') to a user machine. That is, the public key certificate of the shop server 100 and the public key certificate of the user machine authentication server 300 are attached to the data which added the

signature of a shop server to the simplified encryption contents key data (DAS) which are shown in drawing 34 (j'), and it sends to the user machine 200.
[0193] (18) From the received-data verification shop server 100, the user machine 200 which received the encryption contents key data 2 (shop) performs verification processing of the encryption contents key data 2 (shop). This verification processing is the same processing as the processing flow of drawing 15 explained previously, and the user machine 200 performs verification of the public key certificate of the shop server first received from the shop server 100 using the public key KpCA of an issue office (CA), and performs verification of the electronic signature of the encryption contents key data 2 (shop) shown in drawing 33 (k) using the public key KpSHOP of the shop server 100 picked out from the public key certificate next. Furthermore, verification of the public key certificate of the user machine authentication server 300 is performed using the public key KpCA of an issue office (CA), and signature verification of (11) encryption contents key data (DAS) contained in the encryption contents key data 2 (shop) shown in drawing 33 (j) using the public key KpDAS of the user machine authentication server 300 picked out from the public key certificate next is performed. Furthermore, you may make it verify the encryption contents key 1 (shop 1) in the encryption contents data (DAS) of drawing 33 (j) if needed.
[0194] (19) The user machine 200 which verified the encryption contents key data 2 (shop) received from the preservation processing shop server 100 Encryption contents key:KpDEV (Kc) enciphered with the self public key KpDEV contained in the encryption contents key data 2 (shop) is decoded using the self private key KsDEV. Furthermore, it enciphers using the preservation key Ksto of a user machine, encryption contents key:Ksto (Kc) is generated, and this is stored in the storage means of the user machine 200. Encryption contents key:Ksto (Kc) is decoded using the preservation key Ksto, using the contents key Kc which took out and took out the contents key Kc, in the utilization time of contents, decode processing of the encryption contents Kc (Content) is performed, and contents (Content) are reproduced and performed to it.
[0195] Thus, in the basic distribution model 2, between the user machine 200 and the user machine authentication server 300, transmission and reception of data are not performed but the processing burden of a user machine is mitigated only for the user machine 200 performing data transmission and reception between the shop servers 100.
[0196] [1.2. Modification] of the basic contents distribution model 2, next the modification of the configuration of the basic contents distribution model 2 shown in drawing 31 are explained. The configuration shown in drawing 35 is a configuration of having separated the function of a shop server and having prepared the shop server and the distribution server. Although the shop server 100 receives the contents purchase demand from the user machine 200, the distribution server 400 performs contents distribution to the user machine 200. With this configuration, mutual recognition between the entities which perform data transmission and reception is not performed, but each entity performs only signature verification of received data. However, the configuration which performs mutual recognition processing is not cared about at all between entities like the basic contents distribution model 2.
[0197] After the shop server 100 receives the purchase requested data from the user machine 200, verifies data (processing of drawing 35 (3)) and checks the justification of requested data, it performs transmission of a contents distribution demand to the

distribution server 400 (processing of drawing 35 (4)). The distribution server 400 transmits the encryption contents taken out from the contents database 410, when the contents distribution requested data from the shop server 100 is verified and the justification of data is checked (processing of drawing 35 (6)).
[0198] From the distribution server 400, the user machine 200 receives encryption contents and transmits encryption contents receipt data to the distribution server 400 after data verification (processing of drawing 35 (8)). After received-data verification, the distribution server 400 is obtained to the user machine authentication server 300 in encryption contents key data (distribution server) and an encryption contents key, or **, and transmits a demand (processing of drawing 35 (10)).
[0199] The processing after the user machine authentication server 300 obtained from the distribution server 400 in encryption contents key data (distribution server) and an encryption contents key, or ** and received the demand becomes being the same as that of the example based on the configuration shown in previous drawing 31 except having omitted mutual recognition processing.
[0200] In this configuration, without performing mutual recognition, a user machine transmits a contents purchase demand to a shop server, and receives encryption contents from a distribution server. The shop server 100 receives the contents demand from a user machine, and verifies the justification only based on signature verification. Furthermore, it reapplies from a user machine authentication server, a settled encryption contents key is received, and the justification is performed by signature verification. The distribution server 400 performs signature verification about the received data from a shop server, checks data justification, and performs contents distribution.
[0201] The shop server 100 does not perform management of the contents itself, and distribution. It is a mode suitable for the configuration which transmits a contents distribution demand to the distribution server to which one shop server answers a contents demand from a user machine to two or more distribution servers used as various contents administration, such as a music content distribution server which follows, for example, manages music data, and a game contents distribution server which manages game contents, and a shop server manages demand contents according to a demand. Moreover, since for example, a user machine and a shop server are two-way communication by having made it this configuration, the Internet is used, but from a distribution server, to a user machine, since it is one-way communication, there is a merit which can use high-speed satellite communication.
[0202] In this example, mutual recognition is omitted, and since it considered as the processing which checks the justification of data only by signature verification, the increase in efficiency of processing is realized.
[0203] Drawing 36 separates the function of a shop server like drawing 35 , and prepares a shop server and a distribution server, and it is the configuration of having omitted mutual recognition, and the shop server 100 receives the contents purchase demand from the user machine 200, and performs signature verification. The distribution server 400 performs contents distribution to the user machine 200. A different point from the configuration of drawing 35 is a point considered as the configuration to which a contents distribution demand is not transmitted from the shop

server 100 to the distribution server 400, but the user machine authentication server 300 transmits a contents distribution demand to the distribution server 400.
[0204] After the shop server 100 receives the purchase requested data from the user machine 200, verifies data (processing of drawing 36 (3)) and checks the justification of requested data, it performs transmission of the encryption contents key data 1 (shop) to the user machine authentication server 300 (processing of drawing 36 (4)). Then, after the user machine authentication server 300 verifies data (processing of drawing 36 (5)) and checks the justification of requested data, it performs transmission of a contents distribution demand to the distribution server 400 (processing of drawing 36 (6)). The distribution server 400 transmits the encryption contents taken out from the contents database 410 to the user machine 200, when the contents distribution requested data from the user machine authentication server 300 is verified and justification is checked (processing of drawing 36 (8)). Future processings become being the same as that of the processing based on the configuration shown in previous drawing 35 .
[0205] In this configuration, when the key from the distribution server 400 reapplies the user machine authentication server 300 and it has a contents purchase demand to the shop server 100 before a demand, it becomes possible [acquiring and managing the user machine information which is a contents purchase demand subject]. Therefore, the key from the distribution server 400 rechips, and collating processing of whether to be a registered contents purchase demand user machine is already attained at the time of demand receipt. Moreover, if it considers that he is the engine which can trust DAS, a distribution server becomes unnecessary to verify the transmit data of a shop server, and can attain the increase in efficiency of processing.
[0206] as mentioned above -- according to [as explained] the contents distribution configuration of this invention -- a user machine -- after encryption contents Kc (Content) acquisition and contents -- until it results in an available condition -- **** -- it obtains in the key or ** of an encryption contents key in a user machine authentication server, and a treatment process becomes indispensable. Therefore, to a user machine, a shop server cannot notify to a user machine authentication server, cannot sell contents, and cannot make contents an available condition in a user machine. A user machine authentication server in a user machine authentication server license management database (refer to drawing 6) All keys, **, or the contents of contents dealings that obtained and performed processing is recorded. Management of dealings of all shops is possible and the charged contents dealings are grasped. It becomes possible to distribute correctly the contents tariff received in the accounting of a shop to various persons concerned, such as a copyright person of contents, a shop, and a user machine authentication server manager, and the configuration which eliminates unjust contents use is realized.
[0207] [2. Based on use (purchase) of the contents by contents distribution model] using an electronic ticket, next the user, the electronic ticket which described the profits allocation information to various persons concerned, such as a copyright person of contents, a manufacturer, a license electrode holder, and a shop, is published, and the configuration which performs profits allocation processing based on the published electronic ticket is explained.
[0208] The system configuration which performs profits allocation based on an electronic ticket to drawing 37 is shown. The contents distribution system of drawing 37

receives the purchase demand of the contents which a user machine purchases. The profits allocation information on the use tariff accompanying contents purchase As the key or ** for the ticket issue server (TIS:Ticket Issuer Server) 610 which publishes the described electronic ticket, the user machine (DEV) 620 which serves as a contents purchase subject, and just contents dealings management, or a management server which processes by obtaining the distribution servers (CP:Content Provider) 640, such as a content provider (CP) who performs distribution of the functioning user machine authentication server (DAS:Device Authentication Server) 630 and contents, -- further Let the ticket liquidation server (TES:Ticket Exchange Server) 650 which performs liquidation processing of the change of a use tariff etc. based on an electronic ticket be the main component.

[0209] (Ticket issue server) The configuration of the ticket issue server (TIS) 610 of the contents distribution system of drawing 37 is shown in drawing 38 . The ticket issue server 610 receives the purchase demand from the user machine 620, and publishes the electronic ticket which described the profits allocation information corresponding to the contents used as the candidate for dealings with a purchase demand.

[0210] The ticket issue server (TIS) 610 has the ticket issue management database 612 which matches and manages the identifier of the management data of the issue ticket accompanying contents dealings, for example, the user machine of a contents sale place, a contents identifier, a contents tariff, etc. Furthermore, it has the control means 613 which performs communications processing with the contents purchase demand verification from the user machine 620, control of a ticket issue management database, the accounting to the user machine based on a ticket, a user machine, etc., data cipher processing further for each communications processing, etc.

[0211] The data configuration of the ticket issue management database 612 is shown in drawing 39 . Ticket issue processing No. as an identification number which carries out internal generation in case, as for the ticket issue management database 612, a ticket issue server performs ticket issue processing according to contents dealings, The device ID which is the identifier of a user machine which published the contents purchase request The transaction ID which carries out generation issue with a user vessel as a contents dealings identifier in case dealings between a user machine and a ticket issue server are performed The content ID which is the identifier of the contents for dealings, the entity which obtains a countervalue based on the electronic ticket which the ticket issue server 610 publishes, For example, the ticket use place ID as identifiers, such as a copyright person, a license holder, a manager, and the contents selling persons concerned It has each information on the status which shows the status of the ticket issue in the amount of money as the contents use tariff allocation amount of money corresponding to each ticket use place ID, the expiration date of the liquidation processing based on a ticket, and the ticket issue server 610, and management processing. The status is updated according to advance of two or more processings accompanying dealings of contents, although the latter part explains to a detail.

[0212] As the control means 613 of the ticket issue server 610 is shown in drawing 38 , it also has a function as a cipher-processing means and a communications processing means, and a control means 613 is constituted by the computer which stored for example, the code processing program and the communication link processing program. The key data used in cipher processing performed in the cipher-processing means of a

control means 613 are stored in the storage means inside a control means secure one. As code problem data, such as a cryptographic key which the ticket issue server 610 stores, there is a public key KpCA of the certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private key:KsTIS of the ticket issue server 610, public key certificate Cert_TIS of the ticket issue server 610, and a public key certificate.

[0213] The configuration of a control means 613 is a configuration with the control means configuration previously explained using drawing 4 , the same configuration (CPU:Central Processing Unit), i.e., arithmetic and program control, ROM (Read only Memory) and RAM (Random Access Memory), a display, the input section, a storage means, a communication interface, etc.

[0214] (User machine) The user machine (DEV) 620 has the user machine in the configuration of drawing 1 , i.e., the configuration of drawing 7 and the same configuration. There is a preservation key Ksto applied as an encryption key at the time of storing the public key KpCA and contents of a certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private key:KsDEV of a user machine, public key certificate Cert_DEV of a user machine, and a public key certificate in storage means, such as a user machine, for example, a hard disk etc., as code problem data, such as a cryptographic key which the user machine 620 stores.

[0215] The purchase management database which the user machine 620 in the system which performs the ticket management configuration of drawing 37 has serves as a data configuration with a ticket function manager. The data configuration of a purchase management database is shown in drawing 40 . The transaction ID which carries out generation issue with a user vessel in case a purchase management database performs contents dealings The ticket issue object ID which is the identifier of a ticket issue object which publishes a ticket with the content ID and contents dealings which are the identifiers of the contents for dealings It has each information on the status which shows the ticket transmission place ID as an identifier of the transmission place entity of the point which transmitted ticket issue processing No. which the ticket issue server 610 sets up, and a ticket, and the status of contents dealings processing [in / further / a user machine]. The status is updated according to advance of two or more processings accompanying dealings of contents, although the latter part explains to a detail.

[0216] (User machine authentication server) The user machine authentication server (DAS) 630 has the user machine authentication server in the configuration of drawing 1 , i.e., the configuration of drawing 5 and the same configuration. As code problem data, such as a cryptographic key which the user machine authentication server 630 stores, there is a public key KpCA of the certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private key:KsDAS of a user machine authentication server (DAS), public key certificate Cert_DAS of a user machine authentication server (DAS), and a public key certificate.

[0217] The license management database which the user machine authentication server 630 in the system which performs the ticket management configuration of drawing 37 has serves as a data configuration with a ticket function manager. The data configuration of a license management database is shown in drawing 41 . User machine authentication server processing No. as a processing identifier in which a license

management database carries out internal generation according to the processing to which the user machine authentication server (DAS) 630 performs at the time of contents dealings, The device ID which is the identifier of a user machine which published the contents purchase request The transaction ID which carries out generation issue with a user vessel in case contents dealings are performed The ticket issue object ID which is the identifier of a ticket issue object which publishes a ticket with the content ID and contents dealings which are the identifiers of the contents for dealings It has each information on ticket issue processing No. which the ticket issue server 610 sets up, and the status which shows the status of the contents dealings processing in a user machine authentication server (DAS) further. The status is updated according to advance of two or more processings accompanying dealings of contents, although the latter part explains to a detail.

[0218] (Distribution server) The configuration of the distribution server 640 of the contents distribution system of drawing 37 is shown in drawing 42 . It is a content provider (CP) and the distribution server 640 has the contents database 644 which stored the encryption contents key KpDAS (Kc) which enciphered the contents key Kc as Kc (Content) which is encryption contents data which enciphered the contents used as the candidate for dealings by the contents key by public key:KpDAS of a user machine authentication server (DAS:Device Authentication Server). In addition, the content ID which is a contents identifier, respectively is added, and Kc (Content) which is encryption contents data has an identifiable configuration based on content ID, as shown also in drawing.

[0219] The distribution server 640 has the distribution management database 642 which manages the distribution management data of contents further. The distribution management database 642 serves as a data configuration with a ticket function manager. The data configuration of a purchase management database is shown in drawing 43 . In case the distribution management database 642 performs contents message distribution processing Distribution server processing No. which the distribution server 640 sets up, the content ID which is the identifier of the contents for dealings, The ticket issue object ID which is the identifier of a ticket issue object which publishes a ticket with the user machine ID as an identifier for distribution of contents, and contents dealings It has each information on ticket issue processing No. which a ticket issue object sets up, and the status which shows the status of the contents dealings processing in a distribution server further. The status is [0220] updated according to advance of two or more processings accompanying dealings of contents although the latter part explains to a detail. Furthermore, the distribution server 640 has the control means 643 which performs extract processing of the distribution contents from the contents database 644, generation processing of the dealings data registered to the distribution management database 642 accompanying dealings, communications processing besides the user machine 620, data cipher processing further for each communications processing, etc. As a control means 643 is shown in drawing 42 , it also has a function as a cipher-processing means and a communications processing means, and a control means 643 is constituted by the computer which stored for example, the code processing program and the communication link processing program. The key data used in cipher processing performed in the cipher-processing means of a control means 643 are stored in the storage means inside a control means secure one.

As code problem data, such as a cryptographic key which the distribution server 640 stores, there is a public key KpCA of the certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private key:KsCP of the distribution server 640, public key certificate Cert_CP of the distribution server 640, and a public key certificate.

[0221] The configuration of a control means 643 is a configuration with the control means configuration previously explained using drawing 4 , the same configuration (CPU:Central Processing Unit), i.e., arithmetic and program control, ROM (Read only Memory) and RAM (Random Access Memory), a display, the input section, a storage means, a communication interface, etc.

[0222] (Ticket liquidation server) The configuration of the ticket liquidation server (TES) 650 of the contents distribution system of drawing 37 is shown in drawing 44 . As a concrete example which the ticket liquidation server 650 receives an electronic ticket from various entities, and performs the liquidation processing based on a ticket, for example, account transfer processing, balance modification processing of cybermoney, etc. after verification of received data, a setup made into the server in the bank which manages the bank account of each entity is possible for the ticket liquidation server 650.

[0223] The ticket liquidation server 650 has the ticket liquidation management database 652 which manages the management data of the liquidation processing based on the issue ticket accompanying contents dealings. Furthermore, it has the control means 653 which performs the receiving ticket verification from each entity, control of a ticket liquidation management database, communications processing with each entity, data cipher processing further for each communications processing, etc.

[0224] The data configuration of the ticket liquidation management database 652 is shown in drawing 45 . Ticket liquidation server processing No. as an identification number which carries out internal generation in case, as for the ticket liquidation management database 652, a ticket liquidation server performs ticket liquidation processing according to a receipt ticket, The liquidation request origin ID as a demand subject identifier which has required the liquidation based on a ticket The ticket issue object ID which is the identifier of a ticket issue object which publishes a ticket with contents dealings Ticket issue processing No. which the ticket issue server 610 sets up, the liquidation amount of money based on a ticket, In case the user machine ID as an identifier of the user machine which is the purchase subject of contents, and contents dealings are performed, it has each information on the transaction ID which carries out generation issue with a user vessel, and the status which shows the status of the liquidation processing in a ticket liquidation server further. The status is updated according to advance of two or more processings accompanying dealings of contents, although the latter part explains to a detail.

[0225] Furthermore, the ticket liquidation server 650 has the control means 653 which performs data generation of the ticket liquidation management database 652, an update process, verification processing of a receipt ticket, communications processing with various entities, data cipher processing further for each communications processing, etc. As a control means 653 is shown in drawing 44 , it also has a function as a cipher-processing means and a communications processing means, and a control means 653 is constituted by the computer which stored for example, the code processing program and the communication link processing program. The key data used in cipher

processing performed in the cipher-processing means of a control means 653 are stored in the storage means inside a control means secure one. As code problem data, such as a cryptographic key which the ticket liquidation server 650 stores, there is a public key KpCA of the certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private key:KsTES of the ticket liquidation server 650, public key certificate Cert_TES of the ticket liquidation server 650, and a public key certificate.

[0226] The configuration of a control means 653 is a configuration with the control means configuration previously explained using drawing 4 , the same configuration (CPU:Central Processing Unit), i.e., arithmetic and program control, ROM (Read only Memory) and RAM (Random Access Memory), a display, the input section, a storage means, a communication interface, etc.

[0227] Processing until return and a user machine publish a contents purchase demand to a ticket issue server, make contents an available condition, it saves in a user vessel and a contents tariff is distributed to [contents purchase processing], next drawing 37 based on a ticket (liquidation) is explained. Processing advances in order of (32) from the number (1) of drawing 37 . The detail of processing is explained to each numerical order.

[0228] (1) The user machine 620 which is going to purchase mutual recognition contents performs mutual recognition processing between the ticket issue servers 610. Mutual recognition processing is the processing explained using drawing 12 or drawing 13 . In mutual recognition processing, using the generated session key, transmit data is enciphered if needed and data communication is performed.

[0229] (2) If the mutual recognition between Transaction ID, purchase requested data generation, and (3) purchase requested data transmitting ticket issue server 610 and the user machine 620 is successful, the user machine 620 will generate the purchase requested data of contents. The configuration of purchase requested data is shown in drawing 46 (m). Purchase requested data has each data of the content ID as an identifier of the transaction ID which the cipher-processing means of the user machine 620 generates based on a random number as the device ID which is the identifier of the user machine 620 which is the demand origin of contents purchase, and an identifier of dealings, and the contents of which a user machine expects purchase further, and the electronic signature of the user machine to these data is added. Furthermore, the public key certificate of a user machine is attached to purchase requested data if needed for signature verification.

[0230] (4) The ticket issue server 610 which received the purchase requested data shown in received-data verification drawing 46 (m) from the user machine 620 performs verification processing of received data. The detail of verification processing is as having explained using drawing 15 previously.

[0231] (5) The accounting (6) electronic-ticket issue (7) electronic-ticket transmitting ticket issue server 610 performs accounting about dealings of contents, and electronic ticket issue processing next. These processings are performed as processing which publishes the electronic ticket within the dealings amount-of-money limit of the user set up based on the user account registered beforehand, for example or a cybermoney account. The published electronic ticket is transmitted to the user machine 620.

[0232] The example of a configuration of an electronic ticket is shown in drawing 47 . Drawing 47 (A) is a data configuration when the tariff allocation place (tariff receipt entity) based on an electronic ticket is single. The ticket use place ID which shows the tariff allocation place (entity) based on the ticket issue object ID, ticket issue processing No., and an electronic ticket The amount of money which shows the tariff distributed based on an electronic ticket, the expiration date of an electronic ticket, That is, a tariff receipt entity contains the term which can perform liquidation (tariff settlement of accounts) processing based on a ticket, and the purchase requested data (refer to drawing 46 (m)) further transmitted from the user machine to the ticket issue server. In addition, data, such as the ticket date of issue, may be added further. The electronic signature of the ticket issue server 610 is added to these data. Furthermore, the public key certificate of a ticket issue server is attached to an electronic ticket if needed for signature verification.
[0233] Drawing 47 (B) is a data configuration in case the tariff allocation place (entity) based on an electronic ticket is plurality, two or more (1-n) storing of the ticket use place ID is carried out, and the amount of money which shows the tariff distributed based on an electronic ticket is stored to 1-n for every ticket use place ID. The entity which receives a tariff based on a ticket receives the amount of money corresponding to self ID.
[0234] In the example of processing of drawing 37 , the ticket issue server 610 publishes the electronic ticket for the content providers (CP) who manage a distribution server, and the electronic ticket for user machine authentication servers (DAS). These ticket issue places differ for every contents, and the author of contents etc. may be contained. A ticket issue server has the table which determined the allocation amount of money as the ticket issue place based on content ID, acquires allocation amount-of-money data from a table with a ticket issue place based on the content ID contained in a contents purchase demand from a user machine, and generates and publishes a ticket.
[0235] (8) The user machine 620 which received the ticket from the received-data verification ticket issue server 610 performs verification processing of a ticket. This verification processing is the same processing as the processing flow of drawing 15 explained previously, and the user machine 620 performs verification of the public key certificate of a ticket issue server using the public key KpCA of an issue office (CA) first, and performs signature verification of a ticket using the public key KpTIS of a ticket issue server picked out from the public key certificate next.
[0236] (9) mutual recognition (10) electronic-ticket (for CP) transmission -- next, the user machine 620 accesses the distribution server 640, and performs mutual recognition processing. If mutual recognition is materialized, the user machine 620 will transmit the electronic ticket for distribution servers (for CP) to the distribution server 640.
[0237] (11) In received-data verification (12) encryption contents and the encryption contents key transmitting distribution server 640, verification of an electronic ticket (for CP) is completed, and if it judges with it being a just electronic ticket without a data alteration, the distribution server 640 will transmit encryption contents and an encryption contents key to a user machine. Encryption contents:Kc (content) as which these enciphered contents by the contents key, and a contents key: It is data containing encryption contents key data:KpDAS (Kc) which enciphered Kc with the public key of the user machine authentication server (DAS) 630.

[0238] (13) A received-data verification (14) mutual recognition (15) electronic ticket (for DAS) and a key, **, or the user machine 620 that obtained and received encryption contents and an encryption contents key from the demand transmitting distribution server 640 performs verification processing of data. After data verification, the user machine 620 accesses the user machine authentication server 630, and performs mutual recognition processing. If mutual recognition is materialized, to the user machine authentication server 630, the user machine 620 will be obtained in the electronic ticket (DAS) and key for user machine authentication servers, or **, and will transmit a demand. It obtains in a key or ** and a demand is the contents key Kc enciphered with the public key of the user machine authentication server which received from the distribution server 640 previously. The contents key which enciphered the encryption contents key KpDAS (Kc) with the public key KpDEV of a user machine, i.e., the processing set to KpDEV (Kc), is required, and it was reexplaining using drawing 1 , and is the same as that of processing.

[0239] (16) Obtain a received-data verification (17) encryption contents key, **, or the user machine authentication server 630 that obtained, reencryption contents key [an electronic ticket (for DAS), and] KpDAS (Kc) applied from processing and the user machine 620, and received the demand in an electronic ticket (for DAS), an encryption contents key, or **, and it performs verification processing of a demand. When it judges with verification being completed, and it being a just electronic ticket without the alteration of data, obtaining in a just key or **, and being a demand, the user machine authentication server 630 Contents key : Decode data:KpDAS(Kc) which enciphered Kc with the public key KpDAS of the user machine authentication server (DAS) 630 with the private key KsDAS of the user machine authentication server 630, and the contents key Kc is acquired. further -- the contents key Kc -- public key [of a user machine]: -- encryption contents key: enciphered by KpDEV -- KpDEV (Kc) is generated. That is, it obtains in the key or ** of KpDAS(Kc) ->Kc->KpDEV (Kc), and processing is performed. This processing is the same as the processing explained using above-mentioned drawing 16 .

[0240] (18) the encryption contents key transmitting (19) received-data verification (20) preservation processing user machine authentication server 630 -- a key or ** -- obtaining -- transmit the generated encryption contents key KpDEV (Kc) to the user machine 620. From the user machine authentication server 630, the user machine 620 which received the encryption contents key KpDEV (Kc) Received-data verification processing is performed. After verification the user machine 620 The encryption contents key KpDEV (Kc) is decoded using the self private key KsDEV, further, it enciphers using the preservation key Ksto of a user machine, encryption contents key:Ksto (Kc) is generated, and this is stored in the storage means of the user machine 620. Encryption contents key:Ksto (Kc) is decoded using the preservation key Ksto, using the contents key Kc which took out and took out the contents key Kc, in the utilization time of contents, decode processing of the encryption contents Kc (Content) is performed, and contents (Content) are reproduced and performed to it.

[0241] (21) The mutual recognition (22) electronic-ticket (for CP) transmitting distribution server 640 accesses the ticket liquidation server 650 after the encryption contents distribution to the user machine 620, and performs mutual recognition processing. If

mutual recognition is materialized, the distribution server 640 will transmit the electronic ticket for distribution servers (for CP) to the ticket liquidation server 650.
[0242] (23) In received-data verification and the liquidation processing ticket liquidation server 650, verification of an electronic ticket (for CP) is completed, and if it judges with it being a just electronic ticket without a data alteration, the ticket liquidation server 650 will perform liquidation processing based on the received electronic ticket (for CP). Liquidation processing is performed as processing which changes the amount of money set as the electronic ticket (for CP) from the account of Manage User of a user machine to a management account or a cybermoney account of the content provider (CP) who manages the distribution server registered beforehand, for example etc. Or a ticket issue server may already carry out as processing which changes the amount of money set as the ticket by a content provider's (CP)'s management account from the ticket issue server management account received as a prepayment deposit from a user. In addition, the ticket liquidation server 650 verifies the expiration date stored in the ticket, and performs tariff settlement-of-accounts processing based on this ticket a condition [it having been checked that it is within an expiration date].
[0243] (24) In the liquidation processing report report ticket liquidation server 650, after the liquidation based on an electronic ticket (for CP) is completed, the ticket liquidation server 650 transmits the report in which it is shown that liquidation processing ended to the distribution server 640.
[0244] The example of a configuration of a liquidation processing report is shown in drawing 46 (n). The ticket liquidation processing ID in which a liquidation processing report is the identifier of ticket liquidation processing each The liquidation request origin ID as a demand subject identifier which has required the liquidation based on a ticket The ticket issue object ID which is the identifier of a ticket issue object which published the ticket with the liquidation amount of money and contents dealings based on a ticket It has data, such as a ticket liquidation processing completing date when liquidation processing was performed in ticket issue processing No. which the ticket issue server 610 sets up, and the ticket liquidation server 650, and the electronic signature of the ticket liquidation server 650 is added to these. Furthermore, the public key certificate of a ticket liquidation server is attached to a liquidation processing report if needed for signature verification.
[0245] (25) The distribution server 640 which received the liquidation processing report from the received-data verification ticket liquidation server 650 performs verification processing of a liquidation processing report. If it is admited by data verification that a report is just, it will be checked that the tariff allocation accompanying the contents dealings to the content provider who is the administration of a distribution server has been completed.
[0246] (26) mutual recognition (27) electronic-ticket (for DAS) transmitting (28) received-data verification, and liquidation -- the same processing as processing [between the above-mentioned distribution server 640 and the ticket liquidation server 650] (21) - (25) is performed based on an electronic ticket (for DAS) between the processing (29) liquidation processing report report (30) received-data verification user machine authentication server 630 and the ticket liquidation server 650.
[0247] (31) Mutual recognition (32) liquidation processing report report (33) received-data verification and the ticket liquidation server 650 transmit the same liquidation

processing report (refer to drawing 46 (n)) to the ticket issue server 610 with having sent to each entity after mutual recognition with the ticket issue server 610, when liquidation processing is performed based on the ticket received from each entity. The ticket issue server 610 performs verification of a liquidation processing report which received from the ticket liquidation server 650, and checks that the liquidation processing about the published ticket has been completed.

[0248] (Status transition in each device) Each entity of the ticket issue server 610 grade shown in drawing 37 opts for the next processing in a series of processings which relate to contents dealings, respectively according to the status which shows a processing state. The status is managed for every contents dealings in a ticket issue management database, a purchase management database of the user machine of drawing 40 , etc. which are shown in drawing 39 .

[0249] First, status transition of the ticket issue server 610 is explained using drawing 48 . Processing is started because the ticket issue server 610 receives the contents purchase requested data from the user machine 620 (it corresponds to processing (3) of drawing 37). The ticket issue server 610 sets the status as "the completion of purchase reception", when the received data from the user machine 620 are verified and it succeeds in verification, and when the judgment by it being a just purchase demand is not made by data verification, processing is stopped, or the same processing and here the after treatment repeated purchase reception processing the number of predetermined times is stopped, and it carries out the status as "purchase reception failure." Only when the status is "the completion of purchase reception", it progresses to degree step.

[0250] If the status changes to "the completion of purchase reception" next, the ticket issue server 610 will consider the status as "the completion of ticket distribution" by transmitting an electronic ticket to the user machine 620 (it corresponding to processing (7) of drawing 37), and receiving the reception response (response) from a user machine. When a reception response (response) is not received, processing is stopped, or after repeating transmitting processing of an electronic ticket the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "ticket distribution failure." Only when the status is "the completion of ticket distribution", it progresses to degree step.

[0251] When the status changes to "the completion of ticket distribution" next, the ticket issue server 610 receives a liquidation processing report from a ticket liquidation server, and performs verification (it corresponds to processing (32) of drawing 37 , and (33)) of a report. When it succeeds in verification, the status is set as "the completion of liquidation processing report reception", and it considers as processing termination. When judgment that it is a just report is not made by report verification, after stopping processing or repeating report reception and verification processing the number of predetermined times the same processing and here, processing is stopped and the status is carried out as "liquidation report reception failure." The ticket issue server 610 performs such a state transition for every contents dealings.

[0252] Next, status transition of the user machine authentication server 630 is explained using drawing 49 . Processing is started because the user machine authentication server 630 receives the encryption contents key KpDAS from the user machine 620 (Kc) (it corresponds to processing (15) of drawing 37). When the user machine

authentication server 630 verifies the received data containing the electronic ticket (DAS) from the user machine 620 and it succeeds in verification When the status is set as "the completion of key reception" and judgment that it is just data is not made by data verification Processing is stopped, or after repeating the reception of encryption contents key data (user machine) the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key reception failure." Only when the status is "the completion of key reception", it progresses to degree step.

[0253] If the status changes to "the completion of key reception" next, the user machine authentication server 630 will presuppose the status "is completed [it obtains in a key or ** and]", when obtain, it performs processing (it corresponds to processing (17) of drawing 37), it obtains in a key or ** and processing is successful, a contents key, **, or. Since it does not assume a key, **, or that obtaining goes wrong, status transition of "obtaining in a key or ** and completing" exists here.

[0254] When the status changes "to obtain in a key or ** and complete" next, the user machine authentication server 630 transmits encryption contents key data (DAS) to the user machine 620 (it corresponds to processing (18) of drawing 37), and receives the data reception response from the user machine 620. When a data reception response is received, the status is set as "the completion of key transmitting", when reception of a data reception response is not made, after stopping processing or repeating transmitting processing of encryption contents key data (DAS) the number of predetermined times the same processing and here, processing is stopped and the status is carried out as "key transmitting failure."

[0255] If the status changes to "the completion of key transmitting" next, to the ticket liquidation server 650, the user machine authentication server 630 will transmit an electronic ticket (for DAS) (it corresponds to processing (27) of drawing 37), and will receive the data reception response from the ticket liquidation server 650. When a data reception response is received, the status is set up to "the completion of ticket liquidation demand transmitting", when reception of a data reception response is not made, processing is stopped, or the same processing and here, after repeating transmitting processing of a ticket liquidation demand the number of predetermined times, processing is stopped, and the status is carried out as "ticket liquidation demand failure."

[0256] If the status changes to "the completion of ticket liquidation demand transmitting" next, the user machine authentication server 630 will receive the liquidation processing report from the ticket liquidation server 650, and will perform verification processing (it corresponds to processing (29) of drawing 37 , and (30)) of a report. When it succeeds in verification, the status is set as "the completion of liquidation processing report reception", and it considers as processing termination. When judgment that it is a just report is not made by report verification, after stopping processing or repeating report reception and verification processing the number of predetermined times the same processing and here, processing is stopped and the status is carried out as "liquidation report reception failure." The user machine authentication server 630 performs such a state transition for every contents dealings.

[0257] Next, status transition of the distribution server 640 is explained using drawing 50 . Processing is started because the distribution server 640 receives the electronic

ticket (for CP) from the user machine 620 (it corresponds to processing (10) of drawing 37). The distribution server 640 sets the status as "the completion of electronic ticket reception", when the received data from the user machine 620 are verified and it succeeds in verification, when judgment that it is just data is not made by data verification, it stops processing, or after it repeats the reception of a ticket the number of predetermined times, stops processing by the same processing and here, and considers the status as "electronic ticket reception failure." Only when the status is "the completion of electronic ticket reception", it progresses to degree step.

[0258] If the status changes to "the completion of electronic ticket reception" next, the distribution server 640 will transmit encryption contents and the encryption contents key data KpDAS (Kc) to the user machine 620 (it corresponds to processing (12) of drawing 37), and will receive the data reception response from the user machine 620. When a data reception response is received, the status is set as "the completion of distribution", when reception of a data reception response is not made, processing is stopped, or the same processing and here, after repeating transmitting processing of encryption contents and the encryption contents key data KpDAS (Kc) the number of predetermined times, processing is stopped, and the status is carried out as "distribution failure."

[0259] If the status changes to "the completion of distribution" next, to the ticket liquidation server 650, the distribution server 640 will transmit an electronic ticket (for CP) (it corresponds to processing (22) of drawing 37), and will receive the data reception response from the ticket liquidation server 650. When a data reception response is received, the status is set up to "the completion of ticket liquidation demand transmitting", when reception of a data reception response is not made, processing is stopped, or the same processing and here, after repeating transmitting processing of a ticket liquidation demand the number of predetermined times, processing is stopped, and the status is carried out as "ticket liquidation demand failure."

[0260] If the status changes to "the completion of ticket liquidation demand transmitting" next, the distribution server 640 will receive the liquidation processing report from the ticket liquidation server 650, and will perform verification processing (it corresponds to processing (24) of drawing 37 , and (25)) of a report. When it succeeds in verification, the status is set as "the completion of liquidation processing report reception", and it considers as processing termination. When judgment that it is a just report is not made by report verification, after stopping processing or repeating report reception and verification processing the number of predetermined times the same processing and here, processing is stopped and the status is carried out as "liquidation report reception failure." The distribution server 640 performs such a state transition for every contents dealings.

[0261] Next, status transition of the user machine 620 is explained using drawing 51 . Processing is started because the user machine 620 transmits purchase requested data to the ticket issue server 610 first (it corresponds to processing (3) of drawing 37). Processing stops, or after repeating purchase demand transmitting processing the number of predetermined times, the same processing and here processing stops, and a user machine 620 carries out the status as "purchase demand transmitting failure", when the status is set up to "the completion of purchase demand transmitting" and the response of the completion of reception from the ticket issue server 610 cannot receive,

if the response [requested data / to the ticket issue server 610 / purchase] of the completion of reception is received. Only when the status is "the completion of purchase demand transmitting", it progresses to degree step.
[0262] If the status changes to "the completion of purchase demand transmitting" next, from the ticket issue server 610, the user machine 620 will receive an electronic ticket (it corresponds to processing (7) of drawing 37 , and (8)), and will verify received data. When it succeeds in verification of the ticket from the ticket issue server 610, the status is set as "the completion of electronic ticket reception", when judgment that it is a just ticket is not made by data verification, processing is stopped, or after repeating ticket reception the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "electronic ticket reception failure." Only when the status is "the completion of electronic ticket reception", it progresses to degree step.
[0263] When the status changes to "the completion of electronic ticket reception" next, to the distribution server 640, the user machine 620 transmits an electronic ticket (it corresponds to processing (10) of drawing 37), and receives a data receiving response. When a data receiving response is received, the status is set as "the completion of electronic ticket transmitting", when not receiving a data receiving response, processing is stopped, or after repeating ticket transmitting processing the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "electronic ticket transmitting failure." Only when the status is "the completion of electronic ticket transmitting", it progresses to degree step.
[0264] If the status changes to "the completion of electronic ticket transmitting" next, from the distribution server 640, with encryption contents, the user machine 620 will receive the encryption contents key KpDAS (Kc), and will perform data verification (it corresponds to processing (12) of drawing 37 , and (13)). When it succeeds in data verification, the status is set as "the completion of key 1 reception", when it does not succeed in data verification, processing is stopped, or after repeating the reception of key data the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key 1 reception failure."
[0265] If the status changes to "the completion of key 1 reception" next, the user machine 620 will transmit an electronic ticket (for DAS), and the encryption contents key KpDAS (Kc) to the user machine authentication server 630 (it corresponds to processing (15) of drawing 37), and will receive a data receiving response. When obtaining the status in "key or **, setting it as completion of demand transmitting", when a data receiving response is received, and not receiving a data receiving response, after stopping processing or repeating transmitting processing of an electronic ticket (for DAS) and the encryption contents key KpDAS (Kc) the number of predetermined times the same processing and here, processing is stopped, the status is obtained in "key or **, and it carries out as demand transmitting failure." The status obtains in "key or **, and only when it is completion of demand transmitting", it progresses to degree step.
[0266] If the status obtains in "key or ** and changes to completion of demand transmitting" next, from the user machine authentication server 630, the user machine 620 will receive the encryption contents key KpDEV (Kc), and will perform data verification (it corresponds to processing (18) of drawing 37 , and (19)). When it succeeds in data verification, the status is set as "the completion of key 2 reception",

and processing is ended. When it does not succeed in data verification, processing is stopped, or after repeating the reception of key data the number of predetermined times, processing is stopped by the same processing and here, and the status is considered as "key 2 reception failure."

[0267] Next, status transition of the ticket liquidation server 650 is explained using drawing 52 . Processing is started because the ticket liquidation server 650 receives the electronic ticket with the right of allocation by the electronic ticket from an entity (it corresponds to processing (22) of drawing 37 , and (27)). The ticket liquidation server 650 sets the status as "the completion of electronic ticket reception", when a receiving ticket is verified and it succeeds in verification, when judgment that it is just data is not made by data verification, it stops processing, or after it repeats the reception of a ticket the number of predetermined times, stops processing by the same processing and here, and carries out the status as "electronic ticket reception failure." Only when the status is "the completion of electronic ticket reception", it progresses to degree step.

[0268] If the status changes to "the completion of electronic ticket reception" next, the ticket liquidation server 650 will perform liquidation processing based on an electronic ticket. The profits allocation entity into which liquidation processing is registered beforehand, for example, the management account of the content provider (CP) who manages a distribution server, Or the processing which changes the amount of money set as the electronic ticket (for CP) to a cybermoney account etc. from the account of Manage User of a user machine, Or a ticket issue server is already performed to a content provider's (CP)'s management account as processing which changes the amount of money set as the ticket from the ticket issue server management account received as a prepayment deposit from a user. When liquidation processing was completed, the status is set as "the completion of liquidation processing" and liquidation processing is not able to be performed, processing is stopped and the status is considered as "liquidation processing failure."

[0269] If the status changes to "the completion of liquidation processing" next, to the entity which has transmitted the ticket, the ticket liquidation server 650 will transmit a liquidation processing report (it corresponds to processing (24) of drawing 37 , and (29)), and will receive the data reception response from each entity. When a data reception response is received, the status is set as "the completion of liquidation report transmitting", and processing is ended. When reception of a data reception response is not made, processing is stopped, or after repeating transmitting processing of a liquidation report the number of predetermined times, processing is stopped by the same processing and here, and the status is carried out as "liquidation report transmitting failure." The ticket liquidation server 650 performs such a state transition for every contents dealings.

[0270] By circulating the ticket published by drawing 53 with a ticket issue object shows the example of a concrete configuration which performs settlement-of-accounts processing of a contents tariff. If there is a contents purchase demand from the user machine 802 to the ticket issue object 801, a ticket issue object will perform accounting about dealings of contents, and electronic ticket issue processing. These processings are performed as processing which publishes the electronic ticket within the dealings amount-of-money limit of the user set up based on the user account registered beforehand, for example or a cybermoney account. In the example shown in drawing

53 , a ticket issue object publishes the electronic ticket of 1,000 cyclotomies to a user machine as a contents purchase price.
[0271] As shown in the drawing upper part, in the example of drawing 53 , the license holder (user machine authentication server) 803 which is the system management person of contents distribution presupposes [the shop as a ticket issue object / 100 yen and a contents manufacturer (distribution server)] that it is the allocation of 300 yen of the contents tariff of 1000 yen a setup to which 600 yen is received, respectively as a charge of contents as a charge of a license as shop profits as a sales commission.
[0272] The ticket issue object 801 which received the purchase demand from a user machine publishes each electronic ticket, when the setting information on the allocation ratio of a contents tariff is searched for from content ID and there are two or more tariff allocation places. In the example of drawing 53 , the electronic ticket which set up the charge of SEISENSU and the allocation tariff of 100 yen to the license holder 803, and the charge of contents and 600 yen ticket to a contents manufacturer are distributed to the user machine 802. The signature of a ticket issue object is generated by the electronic ticket to distribute.
[0273] the user machine 802 -- the license holder 803 and the contents manufacturer 804 -- each electronic ticket is transmitted to each. After the license holder 803 and the contents manufacturer 804 verify the received electronic ticket and check that it is a just ticket, they transmit a ticket to a bank (ticket liquidation server) 805, perform signature verification also in a liquidation server, check that it is a just ticket, and convert each allocation tariff into money (ex. change processing). In addition, signature verification of the ticket performed in a bank (ticket liquidation server) is verification of a signature of the ticket issue object generated to the electronic ticket. Moreover, verification of a user machine signature of the purchase requested data contained in a ticket is also performed.
[0274] Furthermore, it is good also as a configuration whose bank (ticket liquidation server) generate a signature to the contents manufacturer who is the transmitting subject of a ticket, and the transmit data with which a license holder contains an electronic ticket, and performs signature verification also about these signatures.
[0275] With the configuration of drawing 53 , ticket issue object (shop) 801 self is also the configuration of a contents tariff of converting into money by sending the self electronic ticket of 300 cyclotomies to a bank (ticket liquidation server) 805 in part.
[0276] By liquidation processing of each of these electronic tickets, allocation of a contents tariff is performed certainly. The contents manufacturer 804 transmits encryption contents key:KpDAS (Kc) which enciphered the contents key Kc as the encryption contents enciphered with the contents key Kc with the public key KpDAS of a license holder (user machine authentication server) to the user machine 802, after receiving and verifying an electronic ticket from the user machine 802.
[0277] The user machine 802 transmits the encryption contents key KpDAS (Kc) received from the contents maker 804 to the license holder 803 with an electronic ticket (DAS). After verification of an electronic ticket, a license holder is obtained in the key or ** of the encryption contents key KpDAS (Kc), performs processing, enciphers a contents key with the public key KpDEV of a user machine, generates KpDEV (Kc), and transmits it to the user machine 802. The user machine 802 can decode KpDEV (Kc) with the self private key KsDEV, and can obtain the contents key Kc. Moreover, when it

stores a contents key in a device, it enciphers and saves with the preservation key Ksto of self.
[0278] As mentioned above, the ticket published with a ticket issue object is received. A distribution server (ex. contents manufacturer) transmits encryption contents and an encryption contents key to a user machine a condition [it being a just ticket]. On the other hand, a license holder (user authentication device) by having received the electronic ticket similarly and having considered as the configuration which an encryption contents key chips a condition [it being a just ticket], performs ****, and is distributed to a user machine Allocation of a positive contents tariff based on an electronic ticket is performed, and use of contents is attained in a user machine.
[0279] [3. When the fact that contents distribution management], next the user machine by the log collection server purchased contents is accumulated in a user machine as a log and a system management person collects logs explains the contents distribution system which enabled the grasp of the circulation stereo of contents correctly.
[0280] The system configuration of the contents distribution gestalt which has a log recovery system in drawing 54 is shown. the user machine (DEVICE) 902 which receives the contents distribution from the shop server (SHOP) 901 and the shop server 901 which performs distribution service of contents [as opposed to a user machine in the contents distribution system of drawing 54] -- further The log collection server 903 which functions as a log management server for just contents dealings management is used as the main component. With the content provider 905 as a provider of contents Various information, such as use limit information on contents, is generated as a header to the contents offered by the content provider 905. It has further the authoring server 904 with which a shop server is provided, and the certificate authority (CA:Certificate Authority) which publishes a public key certificate (Cert_xxx) to each entity.
[0281] In the configuration of drawing 54 , a content provider 905 and the authoring server 904 are examples of an entity configuration which offer the contents used as the candidate for circulation to the shop server 901, and offer of the circulation contents to a shop server is made not only in the gestalt of drawing 54 but in other various modes. For example, from a content provider, a direct shop server may be provided with contents and a shop server may be provided with contents through two or more service providers from the author who is a holder of contents.
[0282] The example of a configuration of drawing 54 shows a content provider 905 as one example of representation with the right which acquires some contents sales of an entity, in order to make an understanding of explanation of this invention easy. In the example of a configuration of drawing 54 , a content provider 905 can acquire the allocation profits of self certainly according to the check of the contents sales data managed based on the log collected by the log collection server 903. When there is an entity which has other rights of profits allocation, the entity can join the configuration of drawing 54 and can check the allocation profits of self based on the log collected by the log collection server 903.
[0283] In the configuration of drawing 54 , with having explained in the configuration besides drawing 1 , the shop server 901 is the same configuration, has the control section in which cipher processing and communications processing are possible, performs status management accompanying contents dealings processing, and performs the dealings processing sequence in each device. Moreover, a content

provider 905 and the authoring server 904 also have the control section in which cipher processing and communications processing are possible, perform status management accompanying contents dealings processing, and perform the dealings processing sequence in each device.

[0284] (User machine) The user machine 902 is the same as that of the configuration previously explained using drawing 7 , and has the control means 230 (refer to drawing 7) in which cipher processing and communications processing are possible. However, in this example, a control means 230 stores the log data which generated the log data for every contents purchase processing, and was generated in the purchase management database 220.

[0285] It is generated in the user machine 902 and the example of a configuration of the log data stored is shown in drawing 55 . Two examples of log data are shown in drawing 55 . (A) The day entry which shows the shop ID (ID_SHOP) which is the identifier of a shop which conducted the user machine ID (ID_DEV) which is the identifier of content ID and a user machine which is an identifier of the contents from which the user machine 902 acquired the example 1 of a configuration by dealings with the shop server 901, and dealings, and the time of dealings is included, and the signature (Sig.DEV) of the user machine to these data is generated. A log collection server performs verification processing of the electronic signature of the purchase log which receives from a user machine. (B) The example 2 of a configuration is the configuration that the signature (Sig.DEV) of a user machine was generated to selling check data and the receipt time data of contents. Selling check data are data in which having performed sale of the contents which the shop server 901 generates based on the contents purchase demand from the user machine 902 is shown. The latter part explains selling check data further.

[0286] The user machine 902 generates the log data shown in drawing 55 on the occasion of contents purchase processing, and stores it in a user machine. The stored log data is transmitted to the log collection server 903. A user machine transmits the log data accumulated between them at the time of update process activation of the public key certificate of self to the log collection server 903. The latter part explains these processing sequences to a detail using a flow.

[0287] (Log collection server) The log collection server 903 has the configuration shown in drawing 56 . A log collection server has the collection log management database 9031. The collection log management database 9031 is a database which stores the log data (refer to drawing 55) received from various user machines.

[0288] The log collection server 903 has the control means 9032 which performs communications processing with the user machine 902 and shop server 901 grade, data cipher processing further for each communications processing, etc. A control means 9032 has a function as a cipher-processing means and a communications processing means as well as control means, such as a shop server explained previously. The configuration is the same as the configuration explained using drawing 4 . The key data used in cipher processing performed in the cipher-processing means of a control means 9032 are stored in the storage means inside a control means secure one. As code problem data, such as a cryptographic key which the log collection server 903 stores, there is a public key KpCA of the certificate authority (CA:Certificate Authority) as a public key certificate issue station which is the issue engine of private

key:KsLOG of the log collection server 903, public key certificate Cert_LOG of the log collection server 903, and a public key certificate.
[0289] The log collection server 903 performs issue procedure processing of a public key certificate in exchange for the log data receipt from the user machine 902. The public key which received the public key for updating and was received from the user machine 902 is specifically transmitted to a certificate authority 906, the issue demand of the public key certificate of a user machine is performed, the public key certificate which the certificate authority 906 published is received, and it transmits to the user machine 902. The latter part explains this the processing of a series of to a detail using a flow.
[0290] (Contents purchase processing) The processing in this example is classified into A. contents purchase processing B. log transmission and four processings of public key certificate update process C. contents selling preliminary-treatment D. sales check processing as shown in the upper case of drawing 54 . Hereafter, these the processings of each are explained using a flow.
[0291] (A. Contents purchase processing) Contents purchase processing is explained using the flow of drawing 57 and drawing 58 . In drawing 57 and drawing 58 , a user machine is shown in left-hand side, and processing of a shop server is shown in right-hand side. First, as shown in drawing 57 , mutual recognition is performed between a user machine and a shop server at the time of processing initiation (S1501, S1601).
[0292] Mutual recognition processing is performed as processing based on the public key system explained using drawing 13 . In this mutual recognition, it is carried out using the public key certificate with which the expiration date which a certificate authority (CA) 906 publishes was set up, and a user machine is called for as conditions for having a public key certificate within an expiration date to form mutual recognition. Although the latter part explains, an update process of a public key certificate is performed considering transmission of the log to the log collection server 903 as conditions.
[0293] Data communication is performed or the session key (Kses) generated in mutual recognition processing is used for generation processing of an alteration check value (ICV:Integrity Check Value) in which enciphered the transmit data if needed and Kses was used. About generation of ICV, it mentions later.
[0294] If mutual recognition is materialized, a user machine will generate the transaction ID applied in contents dealings based on a random number, and will generate purchase requested data (S1502). The example of a format of purchase requested data is shown in drawing 59 (A).
[0295] It is the configuration which generated the signature (Sig.Dev) of the list price which are the user machine ID (ID_DEV) which is the identifier of content ID and a user machine which is above-mentioned Transaction ID (TID_DEV) and an above-mentioned contents identifier, and a contents price, and a user [as opposed to / including purchase request time further / these data] machine to purchase requested data.
[0296] Furthermore, a user machine generates the alteration check value (ICV1) of purchase requested data, and transmits it to a shop server (S1503). An alteration check value (ICV) is calculated using the Hash Function to the data for an alteration check, and is calculated by ICV=hash (Kicv, C1 and C2, --). Kicv is an ICV generation key. C1 and C2 are the information on the data for an alteration check, and the message

authenticator (MAC:Message authentication Code) of the critical information of the data for an alteration check is used.
[0297] The example of MAC value generation using a DES cipher-processing configuration is shown in drawing 60 . the (target message as shown in the configuration of drawing 60 -- a 8-byte unit -- dividing -- the divided message is hereafter set to) M1, M2, ..., MN -- the exclusive OR of M1 is first carried out to initial value (Initial Value (hereafter referred to as IV)) (the result is set to I1). Next, I1 is put into the DES encryption section, and it enciphers using a key (hereafter referred to as K1) (an output is set to E1). Continuously, the exclusive OR of E1 and M2 is carried out, the output I2 is put in to the DES encryption section, and it enciphers using a key K1 (output E2). Hereafter, this is repeated and encryption processing is performed to all messages. EN which came out at the end serves as a message authenticator (MAC (Message Authentication Code)). In addition, the partial data which constitute the data used as the candidate for verification as a message are usable.
[0298] Such an alteration check value (ICV) of the data for a check is constituted as a MAC value generated using the ICV generation key Kicv. If it will be guaranteed that there is no alteration in data if that there is no alteration compares guaranteed ICV which the data source generated to the data generate time, for example with ICV which the data receiving side generated based on received data and the same ICV is obtained, and ICV(s) differ, it will be judged with there having been an alteration.
[0299] Here, session key:Kses generated as an ICV generation key at the time of mutual recognition is used. A user machine generates the alteration check value (ICV1) of purchase requested data (refer to drawing 59 (A)) with the application of session key:Kses, and transmits purchase requested data +ICV1 to a shop server.
[0300] a shop -- a server -- ICV -- one -- verification -- namely, -- received data -- being based -- a session -- a key -- : -- Kses -- applying -- an alteration -- a check -- a value -- ICV -- one -- ' -- generating -- having received -- ICV -- one -- = -- ICV -- one -- ' -- being materialized -- a ****** -- judging . When materialized, it judges with having no alteration. Furthermore, a shop server performs signature verification (S1603) of purchase requested data. Signature verification is performed using the public key of a user machine. A public key is taken out from public key certificate Cert_DEV of a user machine, and it becomes conditions that it is a public key certificate within an expiration date. The public key certificate with which the expiration date went out is not used for signature verification in a shop server, but serves as the purchase request NG. the check of ICV, and signature verification -- if all are O.K., a shop server will generate selling check data (S1604).
[0301] Selling check data have the data configuration shown in (B) of drawing 59 . It is the entity which a management person is the management entity (SH: system holder) of for example, a contents selling system, and manages the log collection server 903 by drawing 54 the shop ID (ID_SHOP) which is the identifier of the transaction ID (TID_SHOP) which the shop server generated, and a shop, selling time, the management person commission information over contents sale, and here.
[0302] Furthermore, CP (content provider) sales distribution information and this are information which shows allocation of the content provider to the sales of contents. Furthermore, it is the configuration that the signature (Sig.SHOP) of a shop was generated by these data including purchase requested data (refer to drawing 59 (A)).

[0303] Although the selling check data format of drawing 59 (B) is recording only the allocation information on two entities with a content provider (CP) with the management person (SH: system holder) to the sales of contents, in addition when the allocation place entity of contents sales exists, the allocation information on each of those entities is also stored.
[0304] the check of ICV, and signature verification -- if all are O.K. and selling check data are generated (S1604), a shop server will use the session key Kses for the purchase O.K. data containing the message which consents to purchase, will carry out generation addition of the alteration check value (ICV2), and will transmit to a user machine (S1605). The session key Kses is used for the purchase NG data containing the message in which a shop server refuses purchase as the check of ICV and one of signature verification is NG, generation addition of the alteration check value (ICV2) is carried out, and it transmits to a user machine (S1606).
[0305] Furthermore, a shop server transmits selling check data (refer to drawing 59 (B)), the data which generated the alteration check value (ICV3) using the session key Kses to the header (various contents related information including the use information on contents etc.), and contents to a user machine, when purchase O.K. data are transmitted to a user machine (S1607).
[0306] A user machine receives contents and purchase demand response data (O.K. or NG) +ICV2 (S1504), verifies ICV2, and checks a purchase demand response (S1505). When it is (O.K.) in which it was judged with having no data alteration by ICV2, and purchase was accepted Selling check data (refer to drawing 59 (B)) and header (various contents related information including use information on contents etc.) +ICV3 are received (S1506). Verification of ICV3 and signature verification of selling check data are performed, and when all are O.K., ICV4 is generated to the response of the contents reception O.K., and it transmits to a shop server.
[0307] When the judgment of step S1507 is No, in step S1509, ICV4 is generated to the response of the contents reception NG, and it transmits to a shop server.
[0308] A shop server receives the contents reception O.K. or NG+ICV4 (it carries out and ICV4 is verified (S1611), and when the response from a user machine is the contents reception O.K. further, accounting of the contents to a user is performed (S1613).). (S1608) This accounting is processing which receives a contents tariff from a user's dealings account or credit card designated account like a last example. After accounting is completed, ICV5 is generated to an accounting end message, and it transmits to a user machine (S1614). When either step S1611 or the judgment of S1612 is No, in step S1615, ICV5 is generated in an accounting unfinished message, and it transmits to a user machine.
[0309] The user machine which received accounting termination (or unfinished) message +ICV5 performs verification of ICV5, judges whether accounting was completed further with no problems, if it checks that accounting has ended, will generate a purchase log (refer to drawing 55), and will perform use of contents after saving in the memory of a self-device. When either step S1512 or the judgment of S1513 is No, the header received from the shop server in step S1514 and processing which deletes contents are performed.
[0310] Next, a user machine, the key update process performed between log collection servers, and log transmitting processing are explained using drawing 61 and drawing 62.

Processing of a user machine is shown in the left-hand side of drawing 61 and drawing 62, and processing of a log collection server is shown in right-hand side. This processing is performed in case the user machine which purchases contents from a shop server updates the public key certificate of the user machine stored in the user machine. The expiration date is set to the public key certificate of a user machine, and it is necessary to perform an update process for every fixed period. It explains from processing of drawing 61.

[0311] First, a user machine and a log collection server perform mutual recognition (S1521, S1721), and generate a session key. A user machine takes out the purchase log stored in the memory in a user machine device the condition [authentication formation], generates an alteration check value (ICV1) with the session key Kses to a purchase log, and transmits purchase log +ICV1 to a log collection server (S1522).

[0312] A log collection server receives purchase log +ICV1 (S1722), verification of ICV1 is performed (S1723), and, in Verification O.K., a log is saved in a database (S1724). In addition, a log collection server is good also as a configuration which performs verification processing of the electronic signature of the user machine in a purchase log, and checks the existence of a data alteration further. Further, a log collection server generates an alteration check value (ICV2) with the session key Kses to log reception O.K. data, and transmits log receiving-data +ICV2 to a user machine (S1725). When it is the verification NG of ICV1 of step S1723, the session key Kses generates an alteration check value (ICV2) to log receiving NG data, and log receiving NG data +ICV2 is transmitted to a user machine (S1726).

[0313] Log received-data +ICV2 is received (S1523), and when it is the verification O.K. of ICV2, and the log reception O.K. (S1524), a user machine generates the pair of the public key (KpDEV) and private key (KsDEV) for updating (S1525), it carries out generation addition of the alteration check value (ICV3), and transmits it to the generated public key (KpDEV) at a log collection server (S1526).

[0314] a log collection server -- public key (KpDEV) +ICV3 -- from a user machine -- receiving (S1727) -- verification of ICV3 is performed (S1731), and when it is Verification O.K., generation addition of ICV4 to a public key reception O.K. message is carried out, and it transmits to a user machine (S1732). When verification of ICV3 is NG, generation addition of ICV4 is carried out, and it transmits to a user machine at a public key receiving NG message (S1733).

[0315] When a log collection server carries out generation addition of ICV4 to a public key reception O.K. message and it transmits to a user machine (S1732), an issue office (CA) is received. Furthermore, with a receipt public key Issue of a public key certificate is required, the public key certificate (Cert_DEV) with which the user machine was updated is acquired (S1734), generation addition of the alteration check value ICV5 over the updated public key certificate (Cert_DEV) is carried out further, and it transmits to a user machine (S1735).

[0316] After receiving public key receiving result (O.K. or NG) +ICV4, a user machine performs verification of ICV4, when it is the ICV4 verification O.K. and is the public key reception O.K. (S1532), performs reception (S1533) of updated public key certificate +ICV5, and performs verification of ICV5, and verification (S1534) of a public key certificate which received. When any verification is O.K., the public key in a public key certificate is taken out, the comparison (S1535) with the public key which self

transmitted is performed, when in agreement, the private key generated to updating and the received public key certificate are saved in the memory in a user machine (S1536), and elimination processing (S1537) of a log (log [finishing / sending to a log collection server]) is performed.
[0317] When one judgment of steps S1532, S1534, and S1535 is No, an update process of an effective public key certificate is not performed, but processing is ended.
[0318] Next, the contents sales check processing performed between log collection servers with a content provider is explained based on the flow of drawing 63. A log collection server manages the tariff allocation information over 1 or two or more tariff receipt entities of a contents tariff based on the purchase log received from a user machine, and performs response processing based on tariff allocation information according to the sales acknowledge request from a tariff receipt entity. A log collection server can compute the sales of the tariff receipt entity based on the sales of contents from the content ID contained in a purchase log, and the contents tariff allocation information which a log collection server holds beforehand. In addition, when it is the configuration which receives the log which stored the selling check data shown in drawing 55 (B), the sales of a tariff receipt entity can be computed based on the distribution information included in selling check data.
[0319] First, mutual recognition (S1521, S1721) is performed between log collection servers with a content provider, and the session key Kses is generated. A log collection server takes out a content provider's identifier ID_CP from a content provider's (CP)'s public key certificate Cert_CP a condition [formation of mutual recognition] (S1722), and generates the sales data corresponding to ID_CP based on the log information stored in the database (S1723). As mentioned above, a content provider's allocation information is stored in collected log data, and each content provider's allocation tariff is called for based on log data. Furthermore, a log collection server carries out generation addition of the alteration check value ICV1 over sales data, and transmits to a content provider (CP) (S1724).
[0320] Contents pro BAITA (CP) checks that it sells from a log collection server, data +ICV1 is received (S1522), ICV1 is verified, and there is no data alteration, and saves sales (S1523) data in memory (S1524). Verifying ICV1, in with a data alteration, data storage to memory is not performed, but it ends processing. In this case, the sales data demand to a log collection server is performed again.
[0321] Next, the sales report processing performed between a shop server, a log collection server, and a content provider is explained based on drawing 64 and the processing flow of drawing 65. A shop server manages the sales data of contents and performs processing which transmits all the ********** data within a predetermined period, or the sales data for every tariff receipt entity to a log collection server. Drawing 64 is processing which bundles up the sales of the whole contents selling processing which the shop server performed, and is transmitted to a log collection server, and processing of drawing 65 is processing which chooses the sales about the contents which the specific content provider offered, and is transmitted to a content provider during the contents selling processing which the shop server performed.
[0322] It explains from sales package report processing of drawing 64. First, mutual recognition (S1631, S1731) is performed between a shop server and a log collection server, and the session key Kses is generated. A shop server picks out all the sales

data of a predetermined period from a database a condition [formation of mutual recognition], carries out generation addition of the alteration check value ICV1 over all sales data, and transmits to a log collection server (S1632).
[0323] a log collection server -- from a shop server -- all -- sales data +ICV1 is received (S1732), it checks that ICV1 is verified and there is no data alteration (S1733), and sales data are saved in memory (S1734). Verifying ICV1, in with a data alteration, data storage to memory is not performed, but it ends processing. In this case, the sales data demand to a shop server is performed again.
[0324] Specific content provider sales report processing of drawing 65 is explained. First, mutual recognition (S1641, S1741) is performed between a shop server and a content provider, and the session key Kses is generated. A shop server searches sales data based on ID_CP which took out ID_CP which is a content provider's identifier (S1642), and was taken out from a content provider's public key certificate Cert_CP obtained by mutual recognition the condition [formation of mutual recognition], and acquires the sales data of the specific content provider's offer contents (S1643). Furthermore it sells, generation addition of the alteration check value ICV1 over data is carried out, and it transmits to a log collection server (S1644).
[0325] a log collection server -- from a shop server -- all -- sales data +ICV1 is received (S1742), it checks that ICV1 is verified and there is no data alteration (S1743), and sales data are saved in memory (S1744). Verifying ICV1, in with a data alteration, data storage to memory is not performed, but it ends processing. In this case, the sales data demand to a shop server is performed again.
[0326] According to the configuration of this example, it becomes possible to collect contents purchase log data according to an update process of the public key certificate of a user machine, and the system management person (SH:System Holder) who manages a log collection server becomes possible [grasping a contents sales situation certainly]. The public key certificate of a user machine is required in mutual recognition processing with a shop server, and serves as conditions for having the public key certificate with which the effective term was set up to perform contents purchase. Moreover, it will perform with the public key with which verification of the signature added to purchase requested data etc. from a user machine is also taken out from the public key certificate of a user machine, and it is necessary also in signature verification to have the public key certificate with which the effective term was set up. Therefore, it is necessary to have the public key certificate which transmits log data to a log collection server, updates a public key certificate, and has an effective term in order for a user machine to perform contents purchase. The system management person (SH:System Holder) who manages a log collection server can collect certainly the are recording logs for every setting engine by setting up the expiration date of a public key certificate in one month or three etc. months.
[0327] As mentioned above, the log data from a user machine are certainly collected by the log collection server which a system management person manages, and it becomes possible to manage a contents sales situation. Furthermore, based on the sales allocation information in log data, exact allocation is attained to sales profits acquisition rightful claimants, such as a content provider, in contents sales.
[0328] Moreover, in this example, since it considered as the configuration which adds ICV and communicates at transmit data, using the session key Kses generated to the

data which communicate between each entity at the time of mutual recognition as a generation key of an alteration check value (ICV), the safety of commo data will increase further.

[0329] In addition, although the example mentioned above explained as the mutual recognition processing between a user machine and a shop server, signature generation, and a configuration that performs all of signature verification processing, it is good also as a configuration carried out in use of the public key certificate within an expiration date in either as one of processings, i.e., mutual recognition, or signature generation, and a configuration that performs only signature verification processing as it is indispensable.

[0330] [4. The use configuration of the public key certificate which recorded attribute data or attribute certificate use configuration] next the public key certificate which recorded attribute data, or an attribute certificate is explained. For example, in the contents distribution configuration mentioned above, a malicious shop management person becomes a user machine, and clears up, fictitious dealings of contents may be performed or the fictitious contents dealings between shops may be conducted with a content provider. Moreover, when it is the inaccurate server which the partner became a shop server and cleared up when believed that the user machine which is going to perform just dealings is a shop server, a communication link was started, and a contents purchase demand of a shop server partner was performed, for example, transmitting processing of the credit account number was performed, there is a possibility that processing of acquiring the credit account number from a user machine unjustly may be performed. Furthermore, a user machine becomes a shop, clears up and cannot deny possibility of processing performing fictitious sale of contents to other user machines etc., either. If such a situation occurs, it will become difficult for a system management person to grasp an exact contents distribution stereo.

[0331] As a configuration which prevents false deals other than such the regular contents distribution root etc., the public key certificate or attribute certificate use configuration which recorded attribute data is explained hereafter.

[0332] Attribute data is data which identify the classification of the entity which constitutes contents distribution systems, such as a registration authority which performs the issue examination of a user machine (DEVICE), a shop (SHOP), a content provider (CP), a service management person (SH), a public key certificate, and an attribute certificate.

[0333] As an example of a configuration of attribute data, the table showing the contents of attribute data is shown in drawing 66. A different code is assigned to each entity as shown in drawing 66. For example, the issue demand of a public key certificate and an attribute certificate is received from a user machine or a shop, and "0001" is assigned to the service management person as a system holder who collects the license over the contents which circulate on a "0000" contents distribution system in the registration authority which examines as an attribute code. In the example mentioned above, a service management person is an entity which manages the log information collection server which is the entity which manages a key, **, or the user machine authentication server that obtains and performs processing, and collects log information.

[0334] Furthermore, the code of "0004" is assigned to the user machine which purchased and uses "0003" and contents for the contents distribution person who is the

management entity of the distribution server which distributes contents to a user according to "0002" and the demand from a shop (contents vender) at the contents vender as a shop which sells contents to a user machine. In addition, a different code according to the class is assigned to the entity concerning contents distribution. In addition, when not only the configuration that not necessarily assigns one code but a role and the shop where functions differ are located at a shop, a different code is assigned, and even if distinction of each is possible, it is good, and good also as a configuration which also assigns a different attribute code according to a certain category to a user machine.

[0335] The attribute information mentioned above has the configuration included in a public key certificate, and the configuration which publishes a different attribute certificate from a public key certificate, and identifies an attribute with an attribute certificate. The example of a configuration of a public key certificate with attribute information is shown in drawing 67.

[0336] The public key certificate shown in drawing 67 is the identifier of the algorithm used for the version number of a certificate, the serial number of the certificate which a public key certificate issue office (CA) assigns to a certificate user, and electronic signature and a parameter, and an issue office, the expiration date of a certificate, a certificate user's identifier (ex. user machine ID), a certificate user's public key, [0000] further mentioned above, and [0001]. -- Electronic signature is included in attribute information, such as [nnnn], and a pan. The serial number of a certificate is made into a total of 16 bytes of for example, an issue year (4 bytes), the moon (2 bytes), a day (2 bytes), and a serial number (8 bytes). The identifiable identifier which a registration authority defines or a random number, and the serial number may be used for a user name. Or it is good also as a configuration which makes a high-order byte a category and makes a lower byte the serial number.

[0337] Electronic signature is data which generated the hash value with the application of the Hash Function to the whole attribute data in the identifier of the algorithm used for the version number of a certificate, the serial number of the certificate which a public key certificate issue station (CA) assigns to a certificate user, and electronic signature and a parameter, and an issue station, the expiration date of a certificate, a certificate user's identifier, a certificate user's public key, and the list, and were generated using the private key of an issue station to the hash value.

[0338] a public key certificate issue office (CA) updates the public key certificate with which the expiration date went out, and performs creation of the inaccurate person list of [for excluding the user who performed injustice], management, and distribution (this -- RIBOKESHON: -- referred to as Revocation) while it publishes the public key certificate shown in drawing 67.

[0339] On the other hand, in case this public key certificate is used, using the public key KpCA of the issue station which self holds, a user verifies the electronic signature of the public key certificate concerned, after he succeeds in verification of electronic signature, he picks out a public key from a public key certificate, and uses the public key concerned. Therefore, all the users using a public key certificate need to hold the public key of a common public key certificate issue station.

[0340] Next, the data configuration of the public key certificate which does not have attribute information in drawing 68, and an attribute certificate is shown. (A) is a public

key certificate without attribute information, it is the data configuration which removed attribute information from the public key certificate shown in drawing 67, and a public key certificate issue office publishes it. (B) is an attribute certificate. An attribute certificate issue station (AA:Attribute Authority) publishes an attribute certificate.
[0341] The serial number of the public key certificate corresponding to the attribute certificate with which the version number of a certificate and an attribute certificate issue office (AA) publish the attribute certificate shown in drawing 68, and this are the same as that of the serial number of the certificate of a correspondence public key certificate, and it has a function as link data which associate both certificates. The entity which is going to check the attribute of a communications partner with an attribute certificate can check a public key certificate and the attribute certificate to link based on the public key certificate serial number in which it was stored common to a public key certificate and an attribute certificate, and attribute information can be acquired from the attribute certificate which stored the same public key certificate serial number as a public key certificate. The serial number is made into a total of 16 bytes of for example, an issue year (4 bytes), the moon (2 bytes), a day (2 bytes), and a serial number (8 bytes). Furthermore, it is the data configuration which that of the identifier of the algorithm used for electronic signature and a parameter, and an attribute certificate issue office, the expiration date of a certificate, a certificate user's identifier (ex. user machine ID), and this is the same as that of the user name of a corresponding public key certificate, made the category the identifiable identifier which a registration authority defines or a random number, the serial number, or a high-order byte, and made the lower byte the serial number. Furthermore, [0000], [0001] which were mentioned above -- The electronic signature of attribute information, such as [nnnn], and an attribute certificate issue office (AA) is included.
[0342] Electronic signature is data which generated the hash value with the application of the Hash Function to the whole attribute data in the identifier of the algorithm used for the version number of a certificate, the serial number of a public key certificate, and electronic signature and a parameter, and an issue station, the expiration date of a certificate, a certificate user's identifier, and the list, and were generated using the private key of an attribute certificate issue station to the hash value.
[0343] an attribute certificate issue office (AA) updates the attribute certificate with which the expiration date went out, and performs creation of the inaccurate person list of [for excluding the user who performed injustice], management, and distribution (this -- RIBOKESHON: -- referred to as Revocation) while it publishes the attribute certificate shown in drawing 68 (B).
[0344] Drawing which explains to drawing 69 the procedure which publishes newly the user machine which participates in contents dealings, and the public key certificate which a shop server uses, respectively is shown. In addition, the shop server 1010 and the user machine 1020 have the same configuration with above-mentioned drawing 1 etc. having explained here. The service management object 1030 is a system holder (SH) which manages the whole contents distribution, and grasps the circulation situation of contents by the technique of collecting the logs which the contents key mentioned above rechips and are generated by processing or the contents purchase of a user machine. Here, it also has further a function as a registration authority (RA:Registration Authority) which performs reception of an issue demand of a public key certificate

besides the shop server 1010 and the user machine 1020, and an attribute certificate, and an examination. In addition, although it is the configuration in which the service management object 1030 has a function as a system holder (SH), and a function as a registration authority (RA), these may consist of these examples as a separate independent entity.

[0345] By drawing 69, A1-A8 show the new issue procedure of the public key certificate in the user machine 1020, and B1-B7 show the new issue procedure of the public key certificate of the shop server 1010 by it. First, the new issue procedure of the public key certificate in the user machine 1020 is explained.

[0346] (A1) mutual **** -- the user machine 1020 performs mutual recognition between the service management objects 1030 first. However, at this time, since the user machine 1020 does not hold the public key certificate, mutual recognition using a public key certificate cannot be performed, but mutual recognition processing using the symmetry key cipher system previously explained using drawing 12, i.e., a share private key, and an identifier (ID) is performed (see the explanation about drawing 12 for details).

[0347] (A2) If a public key and private key pair generation (A3) public key certificate issue demand (A4) examination & public key certificate issue demand (A5) public key certificate issue demand mutual recognition are materialized, in the cipher-processing section in a self device, the user machine 1020 will generate the pair of the public key registered newly and a private key, and will transmit the generated public key with a certificate issue demand to the service management object 1030. The service management object 1030 which received the public key certificate issue demand examines an issue demand, and when the requirements as an entity which publishes a public key certificate are satisfied, it transmits a certificate issue demand to the public key certificate issue station (CA) 1040. In addition, when it is the public key certificate in which the public key certificate published here has the attribute information shown in drawing 68 (A), the service management object 1030 judges the attribute of the entity which has transmitted the certificate issue demand based on ID.

[0348] The private key as a user machine identifier (ID) and confidential information is beforehand stored in the user machine which participates in contents distribution. These user machine ID and a private key are the configurations managed with the service management object 1030. The service management object 1030 A confidential information storing database is searched based on ID transmitted from a user machine. After checking beforehand that it is the registered user machine ID, only when a private key is taken out, mutual recognition based on a user machine and drawing 12 is performed using this key and it succeeds in mutual recognition, it checks that it is the user machine which can participate in contents distribution.

[0349] (A6) The public key certificate issue office 1040 which received the public key certificate issue demand from the public key certificate issue (A7) public key certificate transmitting (A8) public key certificate transmitting service management object 1030 stores the public key of a user machine, publishes a public key certificate (drawing 67 or drawing 68 (A)) with the electronic signature of the public key certificate issue office 1040, and transmits it to the service management object 1030. The service management object 1030 transmits the public key certificate received from the public key certificate issue station 1040 to the user machine 1020. A user machine stores the

received public key certificate and the private key which generated the point by (A2) in a self-device, and becomes usable at the mutual recognition in the case of contents dealings, data encryption, decode processing, etc.
[0350] On the other hand, although the issue procedure of the public key certificate of the shop server 1010 is the same as the certificate issue procedure in a user machine fundamentally, the procedure which has a shop server approved on the service management object 1030 as an entity which deals with sale of contents is needed. Therefore, it is necessary for the shop server 1010 to perform a license application (procedure of drawing 69 and B-2) with a self public key. It performs that this performs contents sale according to the policy which the service management object 1030 defines as processing which the shop server 1010 accepts. The service management object 1030 can perform contents sale to which the shop server 1010 followed the policy which the service management object 1030 defines, and when it is accepted that the shop server 1010 observes a policy, it advances issue procedure of the public key certificate to a shop. Issue procedure processing of a public key certificate is the same as that of the case of the user machine mentioned above.
[0351] Next, an update process of a public key certificate is explained using drawing 70. As a public key certificate is shown in drawing 67 and drawing 68 (A), the expiration date is set, and since the certificate with which the expiration date passed over the entity which uses a public key certificate cannot be used, an update process is performed within an expiration date and it is necessary to perform issue procedure of the public key certificate with which a new expiration date was set up.
[0352] In drawing 70, A1-A8 show the updating procedure of the public key certificate in the user machine 1020, and B1-B7 show the updating procedure of the public key certificate of the shop server 1010. First, the updating procedure of the public key certificate in the user machine 1020 is explained.
[0353] (A1) mutual **** -- the user machine 1020 performs mutual recognition between the service management objects 1030 first. Since the user machine 1020 holds the public key certificate effective now at this time, mutual recognition using a public key certificate is performed. This is the mutual recognition processing previously explained using drawing 13. In addition, when the expiration date of a public key certificate on hand has already passed, it may be made to perform mutual recognition processing using the share private key previously explained using drawing 12 like new issue procedure, and an identifier (ID).
[0354] (A2) If a new public key and the renewal demand mutual recognition of a renewal demand (A5) of renewal demand (A4) of private key pair generation (A3) public key certificate examination & public key certificate public key certificate are materialized, the user machine 1020 will transmit the public key which generated and generated the pair of the new public key and private key for updating with the renewal demand of a certificate to the service management object 1030 in the cipher-processing section in a self device. The service management object 1030 which received the renewal demand of a public key certificate transmits the renewal demand of a certificate to the public key certificate issue station (CA) 1040, when an updating demand is examined and the requirements for updating are satisfied. In addition, when it is the public key certificate in which the public key certificate published here has the attribute information shown in

drawing 68 (A), the service management object 1030 judges the attribute of the entity which has transmitted the certificate issue demand based on ID.
[0355] (A6) The public key certificate issue office 1040 which received the renewal demand of a public key certificate from the renewal (A7) public key certificate of public key certificate transmitting (A8) public key certificate transmitting service management object 1030 stores the new public key of a user machine, publishes a public key certificate (drawing 67 or drawing 68 (A)) with the electronic signature of the public key certificate issue office 1040, and transmits it to the service management object 1030. The service management object 1030 transmits the public key certificate received from the public key certificate issue station 1040 to the user machine 1020. A user machine stores the received public key certificate and the private key which generated the point by (A2) in a self-device, and becomes usable at the mutual recognition in the case of contents dealings, data encryption, decode processing, etc.
[0356] On the other hand, although the updating procedure of the public key certificate of the shop server 1010 is the same as the renewal procedure of a certificate in a user machine fundamentally, it is necessary to perform renewal of the above-mentioned license application (procedure of drawing 70 and B-2). When the service management object 1030 accepts the renewal of a license of the shop server 1010, updating procedure of the public key certificate to a shop is advanced. Updating procedure processing of a public key certificate is the same as that of the case of the user machine mentioned above.
[0357] Next, the new issue procedure of an attribute certificate is explained using drawing 71. An attribute certificate is a certificate shown in drawing 68 (B), and an attribute certificate is published after issue of the public key certificate shown in drawing 68 (A). By drawing 71, A1-A7 show the new issue procedure of the attribute certificate in the user machine 1020, and B1-B7 show the new issue procedure of the public key certificate of the shop server 1010 by it. First, the new issue procedure of the public key certificate in the user machine 1020 is explained.
[0358] (A1) mutual **** -- the user machine 1020 performs mutual recognition between the service management objects 1030 first. At this time, since the user machine 1020 has already held the public key certificate issue station public key certificate, it performs mutual recognition using a public key certificate.
[0359] (A2) Attribute certificate issue demand (A3) If examination & attribute certificate issue demand (A4) attribute certificate issue demand mutual recognition is materialized, the user machine 1020 will transmit an attribute certificate issue demand to the service management object 1030. The service management object 1030 which received the attribute certificate issue demand examines an issue demand, and when the requirements as an entity which publishes an attribute certificate are satisfied, it transmits a certificate issue demand to the attribute certificate issue station (AA) 1050. In addition, the service management object 1030 judges the attribute of the entity which has transmitted the certificate issue demand here based on ID. In the user vessel which takes part in contents distribution as mentioned above, it checks that a user machine identifier (ID) is stored beforehand, these user machine ID is the configuration managed with the service management object 1030, and the service management object 1030 is the user machine which can take part in contents distribution ID transmitted from a user

machine, and by carrying out comparison reference with the registered user machine ID beforehand.
[0360] (A5) The attribute certificate issue office 1050 which received the attribute certificate issue demand from the attribute certificate issue (A6) attribute certificate transmitting (A7) attribute certificate transmitting service management object 1030 stores the attribute information on a user machine, publishes an attribute certificate (drawing 68 (B)) with the electronic signature of the attribute certificate issue office 1050, and transmits it to the service management object 1030. The service management object 1030 transmits the attribute certificate received from the attribute certificate issue station 1050 to the user machine 1020. A user machine stores the received attribute certificate in a self-device, and uses it for the attribute check processing in the case of contents dealings.
[0361] On the other hand, the issue procedure (B1-B7) of the attribute certificate of the shop server 1010 is the same as the certificate issue procedure in a user machine fundamentally. Moreover, the updating procedure of an attribute certificate also turns into new issue procedure and same procedure.
[0362] Next, the contents dealings accompanied by the attribute check processing by the attribute certificate or the attribute check processing using the attribute information stored in the public key certificate are explained.
[0363] The processing configuration which combines with drawing 72 at the time of mutual recognition, and performs attribute check processing is shown. The configuration of drawing 72 is the same as the system configuration of drawing 1 explained previously. That is, let the shop server 1010 which performs sale of contents, the user machine 1020 which performs contents purchase, and the user machine authentication server 1030 be components. Here, the user machine authentication server 1030 is under management of the service management object mentioned above. Processing advances in order of (20) from the number (1) of drawing 72. The detail of processing is explained to each numerical order.
[0364] (1) The user machine 1020 which is going to purchase mutual recognition and attribute check processing contents from the shop server 1010 performs mutual recognition processing between shop servers. Between two means to perform data transmission and reception, it is performed that a partner checks mutually whether you are a right data communication person, and performs required data transfer mutually after that. Check processing of whether a partner is a right data communication person is mutual recognition processing. The configuration which performs encryption processing by using as a share key the session key which performed generation of a session key and was generated at the time of mutual recognition processing, and performs data transmission is one desirable data transfer method. After signature verification of the issue station of a public key certificate, mutual recognition processing of a public key system takes out the public key of a partner mold, and is performed. Please refer to the explanation about above-mentioned drawing 13 for details.
[0365] Furthermore, attribute check processing is performed in this example. The shop server 1010 checks that it is data in which it is shown that the attribute is a user machine, when attribute data is stored in the public key certificate of a communications partner. When attribute data is not stored in the public key certificate, an attribute is checked using an attribute certificate. In an attribute certificate, since the signature is

made using the private key of an attribute certificate issue station, after performing signature verification using public key:KpAA of an attribute certificate issue station, checking that it is a just certificate and the "serial number" and/or "a user (ID)" of an attribute certificate checking whether it is in agreement with the "serial number" in a public key certificate, and/or "a user (ID)", the attribute information in a certificate is checked.

[0366] On the other hand, the user machine 1020 checks that it is data in which it is shown that the attribute is a shop, when attribute data is stored in the public key certificate of a communications partner. When attribute data is not stored in the public key certificate, signature verification is performed about an attribute certificate using public key:KpAA of an attribute certificate issue station, and it checks that it is a just certificate, and after checking whether the "serial number" and/or "a user (ID)" of an attribute certificate are in agreement with the "serial number" in a public key certificate, and/or "a user (ID)", the attribute information in a certificate is checked.

[0367] The shop server 1010 checks that the attribute of a contents purchase demand subject's public key certificate or an attribute certificate is a user machine, and the user machine 1020 checks that the attribute of the public key certificate of a contents purchase demand place or an attribute certificate is a shop, and shifts to subsequent processing.

[0368] The flow of attribute check processing is shown in drawing 73. Drawing 73 (A) is attribute check processing using a public key certificate in case attribute data is stored in the public key certificate, and (B) is attribute check processing in which the attribute certificate was used.

[0369] It explains from the flow of drawing 73 (A). First, in step S2101, mutual recognition processing using a public key certificate is performed (refer to drawing 13), and attribute information is taken out from a partner's public key certificate a condition [authentication having been materialized] (judgment Yes of S2102). When attribute information is just, it judges with (the judgment Yes of S2104), mutual recognition, and the thing in which the attribute check succeeded (S2105), and it shifts to subsequent processing. In addition, when for example, a user machine tends to access a shop server as an attribute is just, and it is going to perform the contents purchase demand, if an attribute is a shop, it will judge with it being just, and if it is the attribute code which shows other than a shop (for example, other user machines), it will judge with it not being just. This judgment processing for example, when performing a contents purchase demand to a shop server The code which was made to contain the step which performs attribute code comparison processing, and was beforehand given to the shop into the contents purchase demand processing sequence (ex. executive program) [0002], The attribute code acquired from the public key certificate or attribute certificate of a communications partner (entity) is compared, if in agreement, it will judge with it being just, and if inharmonious, it will judge with it not being just. Or it is good also as a configuration which displays on a display the attribute code acquired from the public key certificate or attribute certificate of a communications partner (entity), compares the attribute code set as the entity assumed as a communications partner, and the user itself judges. When a judgment is No at steps S2102 and S2104, if mutual recognition and an attribute check are failure, it will judge (S2106), and subsequent processing is stopped.

[0370] By the processing executive program to a shop, the judgment of attribute justification as mentioned above The code [0002] beforehand given to the shop, and the public key certificate of a communications partner (entity), Or a step is performed as processing which compares the attribute code acquired from the attribute certificate. It obtains in the key or ** which a user machine performs to a user machine authentication server. Moreover, in a demand processing activation sequence (ex. program) A step is performed as processing which compares the code [0001] beforehand given to the user machine authentication server with the attribute code acquired from the public key certificate of a communications partner (entity), or the attribute certificate. In addition, also in the communications processing between a shop and a user machine authentication server, a step is performed in the processing sequence (ex. program) which specifies and performs a communications partner by each entity as processing which compares the attribute code beforehand set up as a just communications partner with the attribute code acquired from the public key certificate of a communications partner (entity), or the attribute certificate.
[0371] Next, the flow which applied the attribute certificate of drawing 73 (B) is explained. First, in step S2201, mutual recognition processing using a public key certificate is performed (refer to drawing 13). Verification of a partner's attribute certificate is performed using the public key of an attribute certificate issue station a condition [authentication having been materialized] (S2203). (judgment Yes of S2202) Verification is successful and it is contingent [on what (judgment Yes of S2204) the public key certificate and the attribute certificate to link were checked for based on the public key certificate serial number in which it was stored common to a public key certificate and an attribute certificate]. Attribute information is taken out from the attribute certificate which stored the same public key certificate serial number as a public key certificate (S2205). When attribute information is just, it judges with (the judgment Yes of S2206), mutual recognition, and the thing in which the attribute check succeeded (S2207), and it shifts to subsequent processing. When a judgment is No at steps S2202, S2204, and S2206, if mutual recognition and an attribute check are failure, it will be judged (S2208), and subsequent processing is stopped.
[0372] (2) If Transaction ID, purchase requested data generation and the (3) purchase requested data transmitting above-mentioned shop server 1010, the mutual recognition between the user machines 1020, and an attribute check are successful, the user machine 1020 will generate the purchase requested data of contents. As the shop ID which is the identifier of the shop server 1010 which the configuration of purchase requested data is a configuration shown in drawing 14 (a) explained previously, and is the demand place of contents purchase, and an identifier of dealings It has each data of the transaction ID which the cipher-processing means of the user machine 1020 generates based on a random number, and the content ID as an identifier of the contents of which a user machine expects purchase further, and the electronic signature of the user machine to these data is added.
[0373] (4) The shop server which received the purchase requested data shown in received-data verification drawing 14 (a) from the user machine 1020 performs verification processing of received data. Previously, as explained using drawing 15, verification processing takes out public key:KpDEV of a user machine from a public key certificate after verification of public key certificate Cert_DEV of a user machine, and

verifies the user machine signature of purchase requested data using public key:Kp_DEV of a user machine.
[0374] If verification is judged as there being no alteration of O.K., i.e., purchase requested data, it will judge that received data are just contents purchase requested data. When verification is abortive, purchase requested data is judged to be those with an alteration, and the processing to the purchase requested data is stopped.
[0375] (5) In encryption contents and the encryption contents key data 1 (shop) transmitting shop server 1010, verification of purchase requested data is completed, and if it judges with it being the just contents purchase demand without a data alteration, the shop server 1010 will transmit encryption contents and the encryption contents key data 1 (shop) to a user machine. Encryption contents:Kc (content) which each of these is data stored in the contents database, and enciphered contents by the contents key, and a contents key: It is encryption contents key data:KpDAS (Kc) which enciphered Kc with the public key of the user machine authentication server (DAS) 1030.
[0376] The encryption contents key data 1 (shop) are a configuration shown in drawing 14 (b) explained previously. That is, it has shop processing No. which the shop server 1010 generated with the user machine ID which is the identifier of the user machine 1020 which is the demand origin of contents purchase, purchase requested data (data except the user machine public key certificate of drawing 14 (a)), and contents dealings, and encryption contents key data:KpDAS (Kc), and the electronic signature of the shop server 1010 to these data is added. Furthermore, the public key certificate of the shop server 1010 is attached to the encryption contents key data 1 (shop), and it is sent to the user machine 1020. In addition, in the above-mentioned mutual recognition processing or processing of the before, a shop server public key certificate does not already need to send anew necessarily, when finishing [sending to a user machine side].
[0377] (6) From the received-data verification shop server 1010 to encryption contents : the user machine 1020 which received the encryption contents key data 1 (shop) indicated to be Kc (content) to drawing 14 (b) performs verification processing of the encryption contents key data 1 (shop). This verification processing is the same processing as the processing flow of drawing 15 explained previously, and the user machine 1020 performs verification of the public key certificate of the shop server first received from the shop server 1010 using the public key KpCA of an issue office (CA), and performs verification of a shop signature of the encryption contents key data 1 shown in drawing 14 (b) using the public key KpSHOP of a shop server picked out from the public key certificate next.
[0378] (7) After mutual recognition and the attribute check processing user machine 1020 receive encryption contents:Kc (content) and the encryption contents key data 1 (shop) from the shop server 1010 and finish verification of the encryption contents key data 1 (shop), the user machine 1020 accesses the user machine authentication server 1030, and performs mutual recognition processing and attribute check processing between the user machine 1020 and the user machine authentication server 1030. This processing is performed in the same procedure as the mutual recognition processing between the above-mentioned shop server 1010 and the user machine 1020, and attribute check processing.

[0379] (8) If it obtains in encryption contents key data (user machine) and an encryption contents key, or ** and the mutual recognition between the demand sending-user machine 1020 and the user machine authentication server 1030 and an attribute check are materialized, to the user machine authentication server 1030, the user machine 1020 will be obtained in the encryption contents key KpDAS (Kc), the encryption contents key, or ** which received from the shop server 1010 previously, and will transmit a demand. The configuration of encryption contents key data (user machine) is a configuration shown in drawing 14 (c) explained previously. That is, it has encryption contents key data (data except the shop public key certificate of drawing 14 (b)) which obtained in an encryption contents key or ** and were received from user machine authentication server ID which is the identifier of the user machine authentication server 1030 which is the demand place of a demand, and the shop server 1010, and the electronic signature of the user machine 1020 to these data is added. Furthermore, the public key certificate of the shop server 1010 and the public key certificate of the user machine 1020 are attached to encryption contents key data (user machine), and it is sent to the user machine authentication server 1030. In addition, when the user machine authentication server 1030 has already held the user machine public key certificate and the shop server public key certificate, it is not necessary to necessarily send anew.

[0380] (9) Obtain the user machine authentication server 1030 which obtained from the received-data verification user machine 1020 in encryption contents key data (user machine) and an encryption contents key, or **, and received the demand (drawing 14 (c)) in an encryption contents key or **, and it performs verification processing of a demand. This verification processing is the same processing as the processing flow of drawing 15 explained previously. The user machine authentication server 1030 Verification of the public key certificate of the user machine first received from the user machine 1020 is performed using the public key KpCA of an issue station (CA). Next, verification of the electronic signature of the encryption contents key data (user machine) shown in drawing 14 (c) using the public key KpDEV of the user machine picked out from the public key certificate is performed. Furthermore, verification of the public key certificate of a shop server is performed using the public key KpCA of an issue office (CA), and verification of a shop signature of (5) encryption contents key data 1 contained in the encryption contents key data (user machine) shown in drawing 14 (c) using the public key KpSHOP of a shop server picked out from the public key certificate next is performed. Moreover, when the wording of a telegram which the user machine transmitted is contained during the format shown in drawing 14 (c), verification of the wording of a telegram is performed if needed.

[0381] (10) Obtain in an encryption contents key or ** and set to the processing user machine authentication server 1030. If it judges with it obtaining in the encryption contents key data (user machine) and the encryption contents key, or ** which received from the user machine 1020, and verification of a demand being completed, and it obtaining in a just key or **, and being a demand The encryption contents key with which the user machine authentication server 1030 is contained in encryption contents key data (user machine), Namely, a contents key : Decode data:KpDAS (Kc) which enciphered Kc with the public key KpDAS of the user machine authentication server (DAS) 1030 with the private key KsDAS of the user machine authentication server 1030,

and the contents key Kc is acquired. further -- the contents key Kc -- public key [of a user machine]: -- encryption contents key: enciphered by KpDEV -- KpDEV (Kc) is generated. That is, it obtains in the key or ** of KpDAS(Kc) ->Kc->KpDEV (Kc), and processing is performed.

[0382] As previously explained using drawing 16, this processing from encryption contents key data (user machine) Contents key data enciphered with the public key KpDAS of the user machine authentication server (DAS) 1030 : KpDAS (Kc) is taken out. Next, it is the processing which re-enciphers the contents key Kc which decoded with the private key KsDAS of the user machine authentication server 1030, and acquired the contents key Kc, next was acquired by decode by public key:KpDEV of a user machine, and generates encryption contents key:KpDEV (Kc).

[0383] (11) In mutual recognition and the attribute check processing user machine authentication server 1030, if it obtains in the above-mentioned key or above-mentioned ** of an encryption contents key and processing is completed, the user machine authentication server 1030 will access the shop server 1010, and will perform mutual recognition processing and attribute check processing between the user machine authentication server 1030 and the shop server 1010. This processing is performed in the same procedure as the mutual recognition processing between the above-mentioned shop server 1010 and the user machine 1020, and attribute check processing.

[0384] (12) If the mutual recognition between the encryption contents data sending-user machine authentication server 1030 and the shop server 1010 and attribute check processing are materialized, the user machine authentication server 1030 will transmit encryption contents key data (DAS) to the shop server 1010. The configuration of encryption contents key data (DAS) is a configuration shown in drawing 17 (d) explained previously. It obtains in Shop ID, encryption contents key data (user machine) (data except the shop of drawing 14 (c), and a user machine public key certificate), and the further above-mentioned key or ** that is the identifier of the shop server 1010 which is the demand place of contents purchase, and has encryption contents key data:KpDEV (Kc) which the user machine authentication server 1030 generated by processing, and the electronic signature of the user machine authentication server 1030 to these data is added. Furthermore, the user machine authentication server 1030 and the public key certificate of the user machine 1020 are attached to encryption contents key data (DAS), and it is sent to the shop server 1010. In addition, when a shop server is already possession ending, it does not necessarily need to send these public key certificates anew.

[0385] Moreover, when it is the existence accepted to be the independent organization which can trust the user machine authentication server 1030 Without considering as the data configuration which contains (8) encryption contents key data (user machine) which the user machine generated as it is, as shown in drawing 17 (d), as shown in drawing 18 (d'), encryption contents key data (DAS) The user machine authentication server 1030 extracts each data of the contents key KpDEV (Kc) enciphered with the public key of the user machine ID, Transaction ID, content ID, the shop processing NO, and a user device. A signature is added to these and it is good also as encryption contents key data (DAS). In this case, since verification of (8) encryption contents key

data (user machine) becomes unnecessary, the public key certificate to attach is good only with the public key certificate of the user machine authentication server 1030.
[0386] (13) The shop server 1010 which received encryption contents key data (DAS) (drawing 17 (d)) from the received-data verification user machine authentication server 1030 performs verification processing of encryption contents key data (DAS). This verification processing is the same processing as the processing flow of drawing 15 explained previously. The shop server 1010 Verification of the public key certificate of the user machine authentication server first received from the user machine authentication server 1030 is performed using the public key KpCA of an issue station (CA). Next, verification of the electronic signature of the encryption contents key data (DAS) shown in drawing 17 (d) using the public key KpDAS of the user machine authentication server 1030 picked out from the public key certificate is performed. Furthermore, verification of the public key certificate of a user machine is performed using the public key KpCA of an issue office (CA), and verification of a user machine signature of (8) encryption contents key data (user machine) contained in the encryption contents key data (DAS) shown in drawing 17 (d) using the public key KpDEV of the user machine picked out from the public key certificate next is performed. Moreover, when the wording of a telegram which the user machine transmitted is contained during the format shown in drawing 14 (c), verification of the wording of a telegram is performed if needed.
[0387] In addition, when the shop server 1010 receives the encryption contents key data (DAS) which were explained previously and which drawing 18 (d') simplified The shop server 1010 performs verification of the public key certificate of a user machine authentication server using the public key KpCA of an issue station (CA). Next, it becomes processing of only performing verification of the electronic signature of the encryption contents key data (DAS) shown in drawing 18 (d') using the public key KpDAS of the user machine authentication server 1030 picked out from the public key certificate.
[0388] (14) Mutual recognition and attribute check (15) encryption contents key requested data transmission, next the user machine 1020 transmit encryption contents key requested data to a shop server. In addition, when performing a demand in a different session from a pre- demand in this case, mutual recognition and an attribute check are performed again, and encryption contents key requested data is transmitted to the shop server 1010 from the user machine 1020 a condition [mutual recognition and an attribute check having been materialized]. Moreover, when the wording of a telegram which the user machine transmitted is contained during the format shown in drawing 14 (c), verification of the wording of a telegram is performed if needed.
[0389] The configuration of encryption contents key requested data is as being shown in drawing 17 (e). Encryption contents key requested data as the shop ID which is the identifier of the shop server 1010 which is the demand place of contents purchase, and an identifier of dealings The transaction ID which the cipher-processing means of the user machine 1020 generates based on a random number Furthermore, the content ID as an identifier of the contents of which a user machine expects purchase, Furthermore, it has shop processing No. contained in the data (refer to drawing 14 (b)) which the shop generated previously and have been transmitted to the user machine 1020 as encryption contents key data 1 (shop), and the electronic signature of the user machine

to these data is added. Furthermore, the public key certificate of a user machine is attached to encryption contents key requested data, and it is sent to the shop server 1010. In addition, a public key certificate does not necessarily need to send anew, when finishing [the storage to a shop side] already.

[0390] (16) Verification processing and the shop server 1010 which received (17) accounting encryption contents key requested data from the user machine perform verification processing of encryption contents key requested data. This is the processing same with having explained using drawing 15. If data verification ends, the shop server 1010 will perform accounting about dealings of contents. Accounting is processing which receives a contents tariff from a user's dealings account. The received contents tariff is distributed to various persons concerned, such as a copyright person of contents, a shop, and a user machine authentication server manager.

[0391] By the time it results in this accounting, since the treatment process is indispensable, the shop server 1010 cannot perform accounting by processing only between user machines by obtaining in the key or ** of an encryption contents key by the user machine authentication server 1030. Moreover, since decode of an encryption contents key cannot be performed in the user machine 1020, use of contents cannot be performed. The contents of contents dealings which the user machine authentication server obtained in all keys or ** in the user machine authentication server license management database explained using drawing 6, and performed processing are recorded, and the grasp of the contents dealings used as all the candidates for accounting is attained. Therefore, the contents dealings by the shop side independent become impossible, and an unjust contents sale is prevented.

[0392] (18) After the accounting in the encryption contents key data 2 (shop) transmitting shop server 1010 is completed, the shop server 1010 transmits the encryption contents key data 2 (shop) to the user machine 1020.

[0393] The configuration of the encryption contents key data 2 (shop) is as being shown in drawing 17 (f) explained previously. It has encryption contents key data (DAS) (data except the user machine of drawing 17 (d), and a user machine authentication server public key certificate) received from the user machine ID which is the identifier of the user machine 1020 which is the demand origin of an encryption contents key demand, and the user machine authentication server 1030, and the electronic signature of the shop server 1010 to these data is added. Furthermore, the public key certificate of the shop server 1010 and the public key certificate of the user machine authentication server 1030 are attached to the encryption contents key data 2 (shop), and it is sent to the user machine 1020. In addition, when the user machine 1020 has already held the user machine authentication server public key certificate and the shop server public key certificate, it is not necessary to necessarily send anew.

[0394] In addition, when it is the existence accepted to be the independent organization which can trust the user machine authentication server 1030 and the encryption contents key data (DAS) which the shop server 1010 receives from the user machine authentication server 1030 are encryption contents key data (DAS) which were explained previously and which drawing 18 (d') simplified, the shop server 1010 sends the encryption contents key data 2 (shop) shown in drawing 18 (f') to a user machine. That is, the public key certificate of the shop server 1010 and the public key certificate of the user machine authentication server 1030 attach to the data which added the

signature of a shop server to the simplified encryption contents key data (DAS) which are shown in drawing 18 (d'), and it sends to the user machine 1020.
[0395] (19) From the received-data verification shop server 1010, the user machine 1020 which received the encryption contents key data 2 (shop) performs verification processing of the encryption contents key data 2 (shop). This verification processing is the same processing as the processing flow of drawing 15 explained previously, and the user machine 1020 performs verification of the public key certificate of the shop server first received from the shop server 1010 using the public key KpCA of an issue office (CA), and performs verification of the electronic signature of the encryption contents key data 2 (shop) shown in drawing 17 (f) using the public key KpSHOP of the shop server 1010 picked out from the public key certificate next. Furthermore, verification of the public key certificate of the user machine authentication server 1030 is performed using the public key KpCA of an issue office (CA), and signature verification of (12) encryption contents key data (DAS) contained in the encryption contents key data 2 (shop) shown in drawing 17 (f) using the public key KpDAS of the user machine authentication server 1030 picked out from the public key certificate next is performed. Moreover, when a certain transmitted wording of a telegram is contained during the format shown in drawing 17 (f), verification of the wording of a telegram is performed if needed.
[0396] (20) The user machine 1020 which verified the encryption contents key data 2 (shop) received from the preservation processing shop server 1010 Encryption contents key:KpDEV (Kc) enciphered with the self public key KpDEV contained in the encryption contents key data 2 (shop) is decoded using the self private key KsDEV. Furthermore, it enciphers using the preservation key Ksto of a user machine, encryption contents key:Ksto (Kc) is generated, and this is stored in the storage means of the user machine 1020. Encryption contents key:Ksto (Kc) is decoded using the preservation key Ksto, using the contents key Kc which took out and took out the contents key Kc, in the utilization time of contents, decode processing of the encryption contents Kc (Content) is performed, and contents (Content) are reproduced and performed to it.
[0397] As stated, in each processing in accordance with contents distribution, as mentioned above, each entity which performs a communication link Since it considered as the configuration which performs processing according to an attribute check after checking that it is, a partner's attribute, for example, user machine Unjust contents dealings, for example, a shop, become a user machine, and it clears up, and it becomes processing of trading in contents, or a shop server, it clears up, and processing of acquiring the credit account number from a user machine unjustly is prevented.
[0398] For example, if a user machine is checked according to an attribute check as the communications partner of a user machine is a shop, it feels easy about the processing accompanying the contents purchase as processing to a shop, can perform it, and if it is checked that a communications partner is a user machine authentication server in an attribute check, the processing to a user machine authentication server, for example, a key, recovers it, and it can perform transmission of a demand. Since the check of the attribute of a communications partner is attained by performing an attribute check according to this configuration, just processing according to each communications partner is performed. Furthermore, since it becomes without transmitting to an inaccurate communications partner accidentally [restricted data], prevention of a data leakage is also possible.

[0399] Next, the partner check by mutual recognition processing is not performed, but only signature verification of received data is performed, and the gestalt which performs an attribute check and performs contents dealings processing is explained to be the existence of a data alteration using drawing 74.
[0400] Processing shown in drawing 74 is performed as processing which excluded mutual recognition processing from the processing shown in drawing 72. Processing advances in order of (16) from the number (1) of drawing 74. The detail of processing is explained to each numerical order.
[0401] (1) Transaction ID, purchase requested data generation and (2) purchase requested data transmitting ****, and the user machine 1020 generate the purchase requested data of contents, and transmit it to the shop server 1010. The configuration of purchase requested data is a configuration shown in drawing 14 (a) explained previously.
[0402] (3) The shop server which received the purchase requested data shown in received-data verification drawing 14 (a) from the user machine 1020 performs verification processing of received data. The check of attribute information also performs verification processing in this example collectively with the check of the alteration existence of purchase requested data.
[0403] A received-data verification processing flow in case attribute information is stored in drawing 75 at the public key certificate is shown. First, the shop server 1010 which received the message, the signature (purchase requested data), and the public key certificate of a user machine (S2301) verifies the public key certificate of a user machine using the public key KpCA of a public key certificate issue station (S2302). If verification is materialized (it is Yes at S2303), public key:KpDEV of a user machine will be taken out from a public key certificate (S2304), and the user machine signature of purchase requested data will be verified using ** and public key:KpDEV of a user machine (S2305). Furthermore, if verification is successful (it is Yes at S2306), attribute information is taken out from a public key certificate (S2307), and it judges whether they are ** and a just attribute (attribute which shows a user machine here) (S2308), and when just, it will shift to the next processing as a verification processing success (S2309). When a judgment is No at steps S2303, S2306, and S2308, processing is stopped as verification processing failure (S2310).
[0404] Next, the received-data verification processing using a public key certificate and an attribute certificate is explained using the flow of drawing 76. First, the shop server 1010 which received the message, the signature (purchase requested data), the public key certificate of a user machine, and the attribute certificate (S2401) verifies the public key certificate of a user machine using the public key KpCA of a public key certificate issue station (S2402). If verification is materialized (it is Yes at S2403), public key:KpDEV of a user machine will be taken out from a public key certificate (S2404), and the user machine signature of purchase requested data will be verified using ** and public key:KpDEV of a user machine (S2405). Furthermore, a success (it is Yes at S2406) of verification verifies an attribute certificate using the public key KpAA of an attribute certificate issue office (S2407). Attribute information is taken out from an attribute certificate a condition [verification having been successful (it being Yes at S2408)] (S2409), and it judges whether they are ** and a just attribute (attribute which shows a user machine here) (S2410), and when just, it shifts to the next processing as

a verification processing success (S2411). When a judgment is No at steps S2403, S2406, S2408, and S2410, processing is stopped as verification processing failure (S2412).
[0405] (4) In encryption contents and the encryption contents key data 1 (shop) transmitting shop server 1010, verification of purchase requested data is completed, and if it is judged with it being the just contents purchase demand without a data alteration and an attribute is checked, the shop server 1010 will transmit encryption contents and the encryption contents key data 1 (shop) (refer to drawing 14 (b)) to a user machine.
[0406] (5) From the received-data verification shop server 1010 to encryption contents : the user machine 1020 which received the encryption contents key data 1 (shop) indicated to be Kc (content) to drawing 14 (b) performs verification processing of the encryption contents key data 1 (shop) and attribute check processing. This verification processing is the same processing as the processing flow of drawing 75 or drawing 76 explained previously. In this case, processing will be stopped when the attribute of a public key certificate or an attribute certificate does not show the shop.
[0407] (6) Obtain in encryption contents key data (user machine) and an encryption contents key, or **, and to the user machine authentication server 1030, obtain demand transmission, next the user machine 1020 in the encryption contents key KpDAS (Kc), the encryption contents key, or ** which received from the shop server 1010 previously, and they transmit a demand (refer to drawing 14 (c)).
[0408] (7) Obtain the user machine authentication server 1030 which obtained from the received-data verification user machine 1020 in encryption contents key data (user machine) and an encryption contents key, or **, and received the demand (drawing 14 (c)) in an encryption contents key or **, and it performs verification processing of a demand. This verification processing is the same processing as drawing 75 explained previously and the processing flow of drawing 76, and is processing which also performs an attribute check collectively. In this case, processing is stopped when the attribute of a public key certificate or an attribute certificate is not a user machine.
[0409] (8) Obtain in an encryption contents key or **, in processing, next the user machine authentication server 1030, obtain in the key or ** of KpDAS(Kc) ->Kc->KpDEV (Kc), and perform processing.
[0410] (9) Encryption contents data transmission, next the user machine authentication server 1030 transmit encryption contents key data (DAS) to the shop server 1010. The configuration of encryption contents key data (DAS) is a configuration shown in drawing 17 (d) explained previously.
[0411] (10) The shop server 1010 which received encryption contents key data (DAS) (drawing 17 (d)) from the received-data verification user machine authentication server 1030 performs verification processing of encryption contents key data (DAS). This verification processing is the same processing as drawing 75 explained previously and the processing flow of drawing 76, and it is collectively performed by attribute check. In this case, processing is stopped when the attribute of a public key certificate or an attribute certificate is not a user machine authentication server (service management object).
[0412] (11) Encryption contents key requested data transmission, next the user machine 1020 transmit encryption contents key requested data to a shop server. The

configuration of encryption contents key requested data is as being shown in drawing 17 (e).
[0413] (12) Verification processing and the shop server 1010 which received (13) accounting encryption contents key requested data from the user machine perform verification processing of encryption contents key requested data. This is the same processing as drawing 75 explained previously and the processing flow of drawing 76, and is processing which also performs an attribute check collectively. In this case, processing is stopped when the attribute of a public key certificate or an attribute certificate is not a user machine. If data verification ends, the shop server 1010 will perform accounting about dealings of contents.
[0414] (14) After the accounting in the encryption contents key data 2 (shop) transmitting shop server 1010 is completed, the shop server 1010 transmits the encryption contents key data 2 (shop) to the user machine 1020. The configuration of the encryption contents key data 2 (shop) is as being shown in drawing 17 (f) explained previously.
[0415] (15) From the received-data verification (16) preservation processing shop server 1010, the user machine 1020 which received the encryption contents key data 2 (shop) performs verification processing of the encryption contents key data 2 (shop). This verification processing is the same processing as drawing 75 explained previously and the processing flow of drawing 76, and is processing which also performs an attribute check collectively. In this case, processing is stopped when the attribute of a public key certificate or an attribute certificate is not a shop. If data verification ends, the user machine 1020 decodes encryption contents key:KpDEV (Kc) enciphered by the preservation processing KpDEV of contents, i.e., a self public key, using the self private key KsDEV, further, it will encipher using the preservation key Ksto of a user machine, and it will generate encryption contents key:Ksto (Kc), and will perform processing which stores this in the storage means of the user machine 1020.
[0416] Thus, in the processing shown in drawing 74, in the signature verification of data which did not perform an attribute check but received at the time of mutual recognition, since it considered as the configuration which performs processing which checks an attribute, processing is simplified and the increase in efficiency of the processing accompanying contents dealings is attained.
[0417] In addition, although the example which applied the attribute check by the attribute data mentioned above explained the configuration which obtains in a key or ** and performs processing in the service management object, it is possible to apply attribute check processing also in the configuration which applied the above-mentioned log collection server, for example. In addition, an attribute is set up based on the function characterized to each entity between the entities which perform general data transmission and reception, and it becomes possible to raise the safety of data communication, and security further by storing the set-up attribute in a public key certificate or an attribute certificate, and performing attribute check processing of a communications partner using these certificates. Moreover, since it combines with the conventional mutual recognition processing and signature verification processing and attribute check processing can be performed, it is [data communication / usual / perform / perform only signature verification or mutual recognition and / if needed / attribute check processing] alternatively possible in signature verification processing,

mutual recognition processing, attribute check processing, or combining and performing according to a security degree.
[0418] As mentioned above, it has explained in detail about this invention, referring to a specific example. However, it is obvious that this contractor can accomplish correction and substitution of this example in the range which does not deviate from the summary of this invention. That is, with the gestalt of instantiation, this invention has been indicated and it should not be interpreted restrictively. In order to judge the summary of this invention, the column of the claim indicated at the beginning should be taken into consideration.
[0419]
[Effect of the Invention] Since it considered as the configuration whose shop server which receives the purchase demand of contents sends the encryption contents key made into the mode in which decode with the storing key of a user machine is possible the condition [the accounting to the contents purchase demand of a user machine having been completed] to a user machine according to the contents distribution system and the contents distribution approach of this invention as having mentioned above, the positive accounting accompanying the purchase of contents becomes possible.
[0420] Furthermore, according to the contents distribution system and the contents distribution approach of this invention It is based on a contents purchase demand from a user machine. Since processing which relocks [which was enciphered with the public key of a user machine authentication server (DAS) / contents / KpDAS] the contents key KpDEV (Kc) enciphered with the public key KpDEV of a user machine (Kc) was considered as the configuration which the user machine authentication server which manages contents distribution performs It enables a user machine authentication server to grasp the contents dealings between a shop and a user machine certainly.
[0421] Furthermore, according to the contents distribution system and the contents distribution approach of this invention, by the data communication performed between a user machine, a shop, and a user machine authentication server, since it considered as mutual recognition processing or signature generation, and the configuration of verification processing that performs either at least, the security of data communication and the check of a data alteration are attained.
DESCRIPTION OF DRAWINGS
[Brief Description of the Drawings]
[Drawing 1] It is drawing explaining the system outline and contents message distribution processing of a contents distribution system of this invention.
[Drawing 2] It is drawing showing the configuration of the shop server in the contents distribution system of this invention.
[Drawing 3] It is drawing showing the configuration of the purchase management database of the shop server in the contents distribution system of this invention.
[Drawing 4] It is drawing showing the control means configuration of the shop server in the contents distribution system of this invention.
[Drawing 5] It is drawing showing the configuration of the user machine authentication server in the contents distribution system of this invention.

[Drawing 6] It is drawing showing the configuration of the license management database of the user machine authentication server in the contents distribution system of this invention.
[Drawing 7] It is drawing showing the configuration of the user machine in the contents distribution system of this invention.
[Drawing 8] It is drawing showing the purchase management database configuration of the user machine in the contents distribution system of this invention.
[Drawing 9] It is drawing showing the public key certificate distribution configuration in the contents distribution system of this invention.
[Drawing 10] It is drawing which explains applicable signature generation processing in the contents distribution system of this invention.
[Drawing 11] It is drawing which explains applicable signature verification processing in the contents distribution system of this invention.
[Drawing 12] It is drawing which explains applicable mutual recognition (symmetry key method) processing in the contents distribution system of this invention.
[Drawing 13] It is drawing which explains applicable mutual recognition (unsymmetrical key method) processing in the contents distribution system of this invention.
[Drawing 14] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 15] It is drawing which explains applicable data verification processing in the contents distribution system of this invention.
[Drawing 16] They are the key or ** performed in the contents distribution system of this invention, or drawing which obtains and explains processing.
[Drawing 17] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 18] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 19] It is drawing explaining the contents key preservation processing performed in the contents distribution system of this invention.
[Drawing 20] It is drawing explaining status changes of the shop server in the contents distribution system of this invention.
[Drawing 21] It is drawing explaining status changes of the user machine in the contents distribution system of this invention.
[Drawing 22] It is drawing explaining status changes of the user machine authentication server in the contents distribution system of this invention.
[Drawing 23] It is drawing showing the processing flow between the shop server in the contents distribution system of this invention, and a user machine (the 1).
[Drawing 24] It is drawing showing the processing flow between the shop server in the contents distribution system of this invention, and a user machine (the 2).
[Drawing 25] It is drawing showing the processing flow between the user machine authentication server in the contents distribution system of this invention, and a user machine.
[Drawing 26] It is drawing showing the processing flow between the user machine authentication server in the contents distribution system of this invention, and a shop server.

[Drawing 27] It is drawing showing the processing flow between the shop server in the contents distribution system of this invention, and a user machine (the 1).
[Drawing 28] It is drawing showing the processing flow between the shop server in the contents distribution system of this invention, and a user machine (the 2).
[Drawing 29] It is drawing explaining the contents message distribution processing using the distribution server as a modification of the contents distribution system of this invention.
[Drawing 30] It is drawing explaining the contents message distribution processing using the distribution server as a modification of the contents distribution system of this invention.
[Drawing 31] It is drawing explaining the contents message distribution processing of the modification of the contents distribution system of this invention.
[Drawing 32] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 33] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 34] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 35] It is drawing explaining contents message distribution processing without mutual recognition of the contents distribution system of this invention.
[Drawing 36] It is drawing explaining the modification of contents message distribution processing without mutual recognition of the contents distribution system of this invention.
[Drawing 37] It is drawing explaining the contents message distribution processing which applied the electronic ticket in the contents distribution system of this invention.
[Drawing 38] It is drawing explaining the configuration of the ticket issue server of the contents distribution system of this invention.
[Drawing 39] It is drawing explaining the ticket issue management database configuration of the ticket issue server of the contents distribution system of this invention.
[Drawing 40] It is drawing explaining the purchase management database configuration of the user machine of the contents distribution system of this invention.
[Drawing 41] It is drawing explaining the license management database configuration of the user machine authentication server of the contents distribution system of this invention.
[Drawing 42] It is drawing explaining the configuration of the distribution server of the contents distribution system of this invention.
[Drawing 43] It is drawing explaining the distribution management database configuration of the distribution server of the contents distribution system of this invention.
[Drawing 44] It is drawing explaining the configuration of the ticket liquidation server of the contents distribution system of this invention.
[Drawing 45] It is drawing explaining the ticket liquidation management database configuration of the ticket liquidation server of the contents distribution system of this invention.

[Drawing 46] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 47] It is drawing explaining the data configuration which communicates between each entity in the contents distribution system of this invention.
[Drawing 48] It is drawing explaining status changes of the ticket issue server in the contents distribution system of this invention.
[Drawing 49] It is drawing explaining status changes of the user machine authentication server in the contents distribution system of this invention.
[Drawing 50] It is drawing explaining status changes of the distribution server in the contents distribution system of this invention.
[Drawing 51] It is drawing explaining status changes of the user machine in the contents distribution system of this invention.
[Drawing 52] It is drawing explaining status changes of the ticket liquidation server in the contents distribution system of this invention.
[Drawing 53] It is drawing explaining the example of the contents message distribution processing which applied the electronic ticket in the contents distribution system of this invention.
[Drawing 54] It is drawing explaining the contents message distribution processing which applied the log collection server in the contents distribution system of this invention.
[Drawing 55] It is drawing explaining the example of a configuration of the purchase log in the contents distribution system of this invention.
[Drawing 56] It is drawing showing the configuration of the log collection server in the contents distribution system of this invention.
[Drawing 57] It is the flow Fig. (the 1) showing processing between shop servers with the user machine in the contents distribution system of this invention.
[Drawing 58] It is the flow Fig. (the 2) showing processing between shop servers with the user machine in the contents distribution system of this invention.
[Drawing 59] It is drawing showing the example of a format of purchase requested data and selling check data in the contents distribution system of this invention.
[Drawing 60] It is drawing in which setting and wearing to the contents distribution system of this invention, or showing a **** alteration check value (ICV) generation processing configuration.
[Drawing 61] It is the flow Fig. (the 1) showing processing between log collection servers with the user machine in the contents distribution system of this invention.
[Drawing 62] It is the flow Fig. (the 2) showing processing between log collection servers with the user machine in the contents distribution system of this invention.
[Drawing 63] It is the flow Fig. showing processing between log collection servers with the content provider in the contents distribution system of this invention.
[Drawing 64] It is the flow Fig. showing processing between the shop server in the contents distribution system of this invention, and a log collection server.
[Drawing 65] It is the flow Fig. showing processing between the shop server in the contents distribution system of this invention, and a log collection server.
[Drawing 66] It is drawing explaining the attribute information applied in the contents distribution system of this invention.

[Drawing 67] It is drawing showing the public key certificate configuration which has applicable attribute information in the contents distribution system of this invention.
[Drawing 68] It is drawing showing an applicable public key certificate and an applicable attribute certificate configuration in the contents distribution system of this invention.
[Drawing 69] It is drawing explaining new issue processing of the public key certificate in the contents distribution system of this invention.
[Drawing 70] It is drawing explaining an update process of the public key certificate in the contents distribution system of this invention.
[Drawing 71] It is drawing explaining new issue processing of the attribute certificate in the contents distribution system of this invention.
[Drawing 72] It is drawing explaining the contents message distribution processing accompanied by the attribute check in the contents distribution system of this invention.
[Drawing 73] It is a flow Fig. explaining the mutual recognition processing accompanied by the attribute check in the contents distribution system of this invention.
[Drawing 74] It is drawing explaining the contents message distribution processing accompanied by the attribute check in the contents distribution system of this invention.
[Drawing 75] It is a flow Fig. explaining the data verification processing accompanied by the attribute check in the contents distribution system of this invention.
[Drawing 76] It is a flow Fig. explaining the data verification processing accompanied by the attribute check in the contents distribution system of this invention.
[Description of Notations]
100 Shop Server
110 Contents Database
120 Purchase Management Database
130 Control Means
131 Control Section
132 ROM
133 RAM
134 Display
135 Input Section
136 HDD
137 Drive
138 Network Interface
200 User Machine
220 Purchase Management Database
230 Control Means
300 User Machine Authentication Server
320 License Management Database
330 Control Means
400 Distribution Server
410 Contents Database
610 Ticket Issue Server
612 Purchase Management Database
613 Control Means
620 User Machine
630 User Machine Authentication Server

640 Distribution Server
642 Distribution Management Database
643 Control Means
644 Contents Database
650 Ticket Liquidation Server
652 Ticket Liquidation Management Database
653 Control Means
801 Ticket Issue Object
802 User Machine
803 License Holder
804 Contents Maker
805 Bank
901 Shop Server
902 User Machine
903 Log Collection Server
904 Authoring Server
905 Content Provider
9031 Log Management Database
9032 Control Means
1010 Shop Server
1020 User Machine
1030 Service Management Object
1040 Public Key Certificate Issue Station
1050 Attribute Certificate Issue Station

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－141895
(P2002－141895A)
(43)公開日　平成14年５月17日(2002.5.17)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｈ０４Ｌ	9/08		Ｇ０６Ｆ 15/00	３３０Ｚ	５Ｂ０８５
Ｇ０６Ｆ	15/00	３３０	17/60	ＺＥＣ	５Ｃ０６４
	17/60	ＺＥＣ		１４２	５Ｊ１０４
		１４２		３０２Ｅ	
		３０２		５１２	

審査請求　未請求　請求項の数18　ＯＬ　(全 86 頁)　最終頁に続く

(21)出願番号　特願2000－334183(P2000－334183)

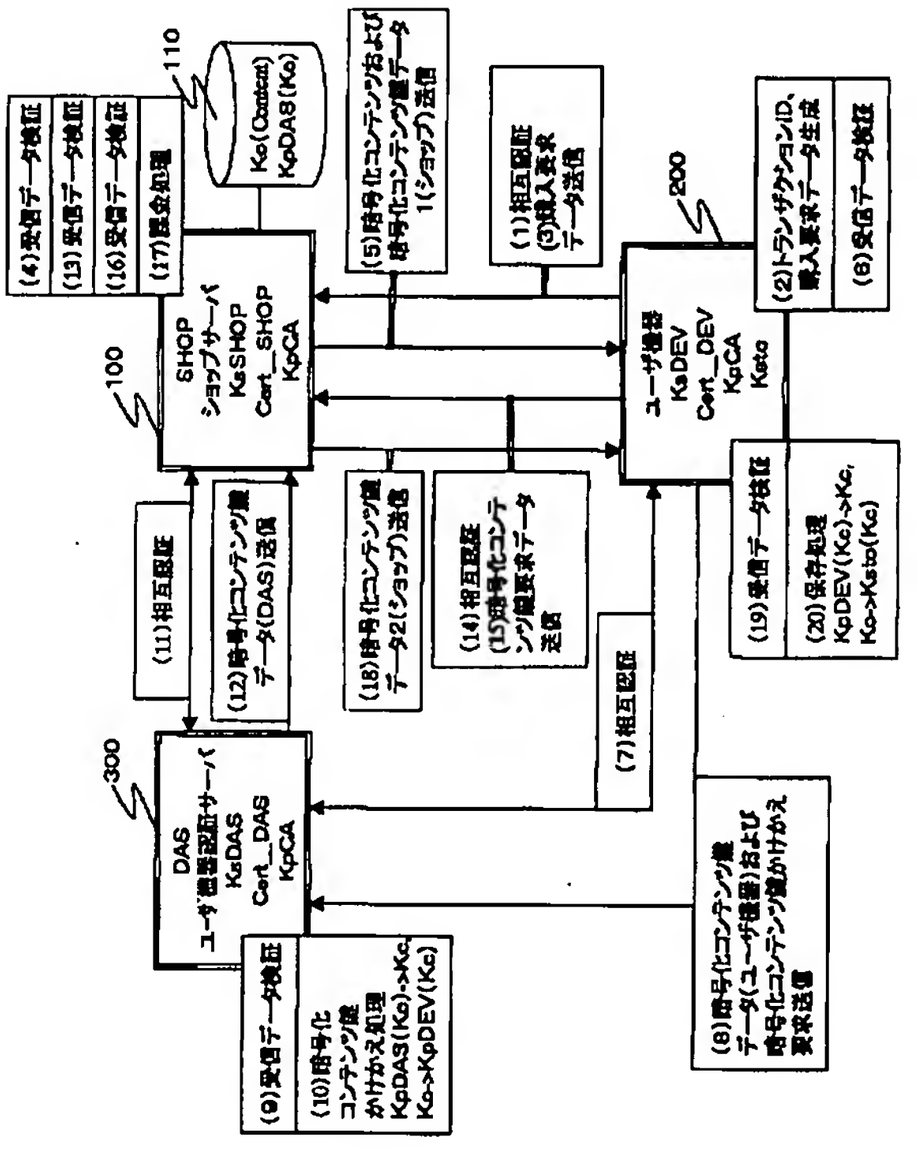
(22)出願日　平成12年11月１日(2000.11.1)

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号
(71)出願人　395015319
株式会社ソニー・コンピュータエンタテインメント
東京都港区赤坂７－１－１
(72)発明者　吉野　賢治
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(74)代理人　100101801
弁理士　山田　英治　(外２名)

最終頁に続く

(54)【発明の名称】　コンテンツ配信システムおよびコンテンツ配信方法

(57)【要約】
【課題】　配信コンテンツの課金処理等の管理を確実にかつ効率的に行なうコンテンツ配信システムを提供する。
【解決手段】　ショップサーバが、ユーザ機器のコンテンツ購入要求に対する課金処理が終了したことを条件として、ユーザ機器の格納鍵での復号可能な態様とした暗号化コンテンツ鍵をユーザ機器に送付する。コンテンツ配信を管理するユーザ機器認証サーバが、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵で暗号化したコンテンツ鍵ＫｐＤＡＳ（Ｋｃ）をユーザ機器の公開鍵ＫｐＤＥＶで暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）にかけかえる処理を実行する。コンテンツ購入要求に対する課金処理が終了したことを条件として、ショップサーバが鍵かけかえ済みのコンテンツ鍵をユーザ機器に送付する。



【特許請求の範囲】
【請求項１】ショップサーバに対してコンテンツ購入要求を送信するユーザ機器（ＤＥＶ）と、
前記ユーザ機器からのコンテンツ購入要求を受信するとともに、コンテンツ鍵Ｋｃで暗号化した暗号化コンテンツと、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵とを管理するショップサーバ（ＳＨＯＰ）と、
前記暗号化コンテンツ鍵を前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵とする鍵かけかえ処理を実行するユーザ機器認証サーバ（ＤＡＳ）とを有し、
前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供する構成としたことを特徴とするコンテンツ配信システム。
【請求項２】前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、
前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項３】前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項４】前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項５】前記コンテンツ配信システムは、さらに、前記ユーザ機器に対して暗号化コンテンツを配信する配信サーバを有し、
前記ショップサーバは、
前記ユーザ機器からのコンテンツ購入要求を受信に応じて、前記配信サーバに対してコンテンツ配信要求を送信する構成を有し、
前記配信サーバは、前記ショップサーバからのコンテンツ配信要求に応じて前記ユーザ機器に対して暗号化コンテンツを配信する処理を実行する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項６】前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、
要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、
前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項７】前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする請求項１に記載のコンテンツ配信システム。
【請求項８】ショップサーバと、ユーザ機器間で取り引きされるコンテンツの配信管理を実行するユーザ機器認証サーバであり、
前記ショップサーバまたは前記ユーザ機器から受領する鍵かけかえ要求の受領に応じて、ショップサーバとユーザ機器間で取り引きされるコンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵から前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵に変換する鍵かけかえ処理を実行する構成を有し、
前記ユーザ機器認証サーバは、前記鍵かけかえ要求中に含まれる前記ショップサーバの電子署名および、前記ユーザ機器の電子署名の検証を行ない、該検証により前記鍵かけかえ要求の正当性が確認されたことを条件として前記鍵かけかえ処理を実行する構成を有することを特徴とするユーザ機器認証サーバ。

【請求項９】ユーザ機器に対して暗号化コンテンツの復号に適用するコンテンツ鍵を提供するショップサーバであり、
コンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵を管理し、
前記ユーザ機器からのコンテンツ購入要求に基づく課金処理の完了を条件として、コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）が前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵の鍵かけかえ処理により生成する前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とするショップサーバ。
【請求項１０】前記ショップサーバは、暗号化コンテンツの配信サーバを含む構成であることを特徴とする請求項９に記載のショップサーバ。
【請求項１１】コンテンツの購入要求を生成しショップサーバに対して送信しコンテンツの再生処理を実行するコンテンツ再生機器であり、
コンテンツの配信管理を行なうユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理により生成される前記コンテンツ再生機器の格納鍵により復号可能な暗号化コンテンツ鍵データをショップサーバを介して受信し、該受信する暗号化コンテンツ鍵データに含まれるショップサーバおよびユーザ機器認証サーバ（ＤＡＳ）の署名検証を実行し、データ改竄の無いことが確認されたことを条件として、受信した暗号化コンテンツ鍵データから暗号化コンテンツ鍵を取り出し復号しコンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ再生機器。
【請求項１２】ユーザ機器（ＤＥＶ）からショップサーバ（ＳＨＯＰ）に対してコンテンツ購入要求を送信するステップと、
ショップサーバ（ＳＨＯＰ）において、前記ユーザ機器からのコンテンツ購入要求を受信するステップと、
ユーザ機器認証サーバ（ＤＡＳ）において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵から、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵へ変換する鍵かけかえ処理を実行するステップと、
前記ショップサーバにおいて前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供するステップと、
を有することを特徴とするコンテンツ配信方法。
【請求項１３】前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、
前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１４】前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１５】前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、
前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１６】前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、
前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理することを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１７】前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステ

ータス情報に基づいて管理することを特徴とする請求項１２に記載のコンテンツ配信方法。
【請求項１８】コンテンツ鍵の配信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、
コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）の生成するユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を受信するステップと、
前記ユーザ機器からのコンテンツ購入要求に基づく課金処理を実行するステップと、
前記課金処理の完了を条件として、前記ユーザ機器に対して、ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を送信するステップと、
を有することを特徴とするプログラム提供媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明はコンテンツ配信システムおよびコンテンツ配信方法に関する。さらに、詳細には、コンテンツ提供サービスを行なうエンティテイと、コンテンツ受信を行なうユーザ機器間におけるコンテンツ取り引きにおけるセキュリティ、管理構成を改善したコンテンツ配信システムおよびコンテンツ配信方法に関する。なお、システムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。
【０００２】
【従来の技術】昨今、ゲームプログラム、音声データ、画像データ、文書作成プログラム等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の、インターネット等、ネットワークを介した流通が盛んになってきている。また、オンラインショッピング、銀行決済、チケット販売等のネットワークを介した商品売買、決済処理等も盛んになってきている。
【０００３】このようなネットワークを介したデータ通信においては、データ送信側とデータ受信側とが互いに正規なデータ送受信対象であることを確認した上で、必要な情報を転送する、すなわちセキュリティを考慮したデータ転送構成をとるのが一般的となっている。データ転送の際のセキュリティ構成を実現する手法には、転送データの暗号化処理、データに対する署名処理等がある。
【０００４】暗号化データは、所定の手続きによる復号化処理によって利用可能な復号データ（平文）に戻すことができる。このような情報の暗号化処理に暗号化鍵を用い、復号化処理に復号化鍵を用いるデータ暗号化、復号化方法は従来からよく知られている。
【０００５】暗号化鍵と復号化鍵を用いるデータ暗号化・復号化方法の態様には様々な種類があるが、その１つの例としていわゆる公開鍵暗号方式と呼ばれる方式がある。公開鍵暗号方式は、発信者と受信者の鍵を異なるものとして、一方の鍵を不特定のユーザが使用可能な公開鍵として、他方を秘密に保つ秘密鍵とするものである。例えば、データ暗号化鍵を公開鍵とし、復号鍵を秘密鍵とする。あるいは、認証子生成鍵を秘密鍵とし、認証子検証鍵を公開鍵とする等の態様において使用される。
【０００６】暗号化、復号化に共通の鍵を用いるいわゆる共通鍵暗号化方式と異なり、公開鍵暗号方式では秘密に保つ必要のある秘密鍵は、特定の１人が持てばよいため鍵の管理において有利である。ただし、公開鍵暗号方式は共通鍵暗号化方式に比較してデータ処理速度が遅く、秘密鍵の配送、ディジタル署名等のデータ量の少ない対象に多く用いられている。公開鍵暗号方式の代表的なものにはＲＳＡ（Rivest-Shamir-Adleman）暗号がある。これは非常に大きな２つの素数（例えば１５０桁）の積を用いるものであり、大きな２つの素数（例えば１５０桁）の積の素因数分解する処理の困難さを利用している。
【０００７】公開鍵暗号方式では、不特定多数に公開鍵を使用可能とする構成であり、配布する公開鍵が正当なものであるか否かを証明する証明書、いわゆる公開鍵証明書を使用する方法が多く用いられている。例えば、利用者Ａが公開鍵、秘密鍵のペアを生成して、生成した公開鍵を認証局に対して送付して公開鍵証明書を認証局から入手する。利用者Ａは公開鍵証明書を一般に公開する。不特定のユーザは公開鍵証明書から所定の手続きを経て公開鍵を入手して文書等を暗号化して利用者Ａに送付する。利用者Ａは秘密鍵を用いて暗号化文書等を復号する等のシステムである。また、利用者Ａは、秘密鍵を用いて文書等に署名を付け、不特定のユーザが公開鍵証明書から所定の手続きを経て公開鍵を入手して、その署名の検証を行なうシステムである。
【０００８】公開鍵証明書は、公開鍵暗号方式における認証局あるいは発行局（ＣＡ：Certificate Authority またはＩＡ：Issuer Authority）が発行する証明書であり、ユーザが自己のＩＤ、公開鍵等を認証局に提出することにより、認証局側が認証局のＩＤや有効期限等の情報を付加し、さらに認証局による署名を付加して作成される証明書である。
【０００９】公開鍵証明書は、証明書のバージョン番号、発行局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前（ユーザＩＤ）、証明書利用者の公開鍵並びに電子署名を含む。
【００１０】電子署名は、証明書のバージョン番号、認証局が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、証明書利用者の名前並びに証明書利用者の公開鍵全体に対しハッシュ関数を

適用してハッシュ値を生成し、そのハッシュ値に対して認証局の秘密鍵を用いて生成したデータである。

【００１１】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する認証局の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の認証局の公開鍵を保持している必要がある。

【００１２】

【発明が解決しようとする課題】上述のような認証局発行の公開鍵証明書を用いた公開鍵暗号方式によるデータ送信システムにおいては、例えばコンテンツを配信するコンテンツ配信ショップは、ユーザの公開鍵に基づいて配信対象のコンテンツを暗号化してユーザに送信する。コンテンツ配信ショップからの暗号化データを受信したユーザ機器は、自己の公開鍵に対応する自己の秘密鍵で暗号化コンテンツの復号を実行する。

【００１３】しかし、現実のコンテンツ取り引きにおいては、コンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者は、コンテンツのユーザに対する提供サービスを行なうコンテンツ配信ショップとは異なる存在である場合が多く、コンテンツを受信しているユーザが、正当なコンテンツ利用権を有しているか否かについては、コンテンツ配信ショップは確認することなくコンテンツの配信を行なっていることが多い。すなわち、正当な利用権を持たないユーザによってコンテンツが不当に利用、あるいは販売される場合がある。

【００１４】また、上記のような取り引き形態においては、コンテンツの販売者であるコンテンツ配信ショップと、コンテンツ利用者であるユーザ機器の２者間においては相応のコンテンツ利用料を伴う取り引きが成立するが、コンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者は、ショップとユーザ間のコンテンツ取り引きに伴うライセンス料の取得が保証されない。現状では、コンテンツ配信ショップの自己申告により、コンテンツの販売量を確認し、自己申告に基づくライセンス料が、ショップからライセンスホルダ、あるいはコンテンツ製作者等に提供されるのが一般的な取り引き形態である。

【００１５】このようなコンテンツ取り引き形態では、コンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者は、コンテンツ取り引きの実体を把握できず、正確な利用権のもとで正当にコンテンツが流通しているか否かを確認する手段がなかった。

【００１６】本発明は、上述のような、コンテンツ取り引きにおける問題点に鑑みてなされたものであり、コンテンツの配信サービスを行なうコンテンツ配信ショップとユーザ間でのコンテンツ取り引きの実体をコンテンツの頒布権を持つライセンスホルダ、あるいはコンテンツの著作権を持つコンテンツ製作者において確実に把握可能とし、正当なコンテンツ利用権の管理のもとでコンテンツ配信を行なう構成としたコンテンツ配信システムおよびコンテンツ配信方法を提供するものである。

【００１７】

【課題を解決するための手段】本発明の第１の側面は、ショップサーバに対してコンテンツ購入要求を送信するユーザ機器（ＤＥＶ）と、前記ユーザ機器からのコンテンツ購入要求を受信するとともに、コンテンツ鍵Ｋｃで暗号化した暗号化コンテンツと、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵とを管理するショップサーバ（ＳＨＯＰ）と、前記暗号化コンテンツ鍵を前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵とする鍵かけかえ処理を実行するユーザ機器認証サーバ（ＤＡＳ）とを有し、前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供する構成としたことを特徴とするコンテンツ配信システムにある。

【００１８】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする。

【００１９】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００２０】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信

し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００２１】さらに、本発明のコンテンツ配信システムの一実施態様において、前記コンテンツ配信システムは、さらに、前記ユーザ機器に対して暗号化コンテンツを配信する配信サーバを有し、前記ショップサーバは、前記ユーザ機器からのコンテンツ購入要求を受信に応じて、前記配信サーバに対してコンテンツ配信要求を送信する構成を有し、前記配信サーバは、前記ショップサーバからのコンテンツ配信要求に応じて前記ユーザ機器に対して暗号化コンテンツを配信する処理を実行する構成を有することを特徴とする。

【００２２】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする。

【００２３】さらに、本発明のコンテンツ配信システムの一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステータス情報に基づいて管理する構成を有することを特徴とする。

【００２４】さらに、本発明の第２の側面は、ショップサーバと、ユーザ機器間で取り引きされるコンテンツの配信管理を実行するユーザ機器認証サーバであり、前記ショップサーバまたは前記ユーザ機器から受領する鍵かけかえ要求の受領に応じて、ショップサーバとユーザ機器間で取り引きされるコンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵から前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵に変換する鍵かけかえ処理を実行する構成を有し、前記ユーザ機器認証サーバは、前記鍵かけかえ要求中に含まれる前記ショップサーバの電子署名および、前記ユーザ機器の電子署名の検証を行ない、該検証により前記鍵かけかえ要求の正当性が確認されたことを条件として前記鍵かけかえ処理を実行する構成を有することを特徴とするユーザ機器認証サーバにある。

【００２５】さらに、本発明の第３の側面は、ユーザ機器に対して暗号化コンテンツの復号に適用するコンテンツ鍵を提供するショップサーバであり、コンテンツの暗号化鍵であるコンテンツ鍵を、前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵を管理し、前記ユーザ機器からのコンテンツ購入要求に基づく課金処理の完了を条件として、コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）が前記ユーザ機器の格納鍵では復号不可能な態様で暗号化した暗号化コンテンツ鍵の鍵かけかえ処理により生成する前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とするショップサーバにある。

【００２６】さらに、本発明のショップサーバの一実施態様において、前記ショップサーバは、暗号化コンテンツの配信サーバを含む構成であることを特徴とする。

【００２７】さらに、本発明の第４の側面は、コンテンツの購入要求を生成しショップサーバに対して送信しコンテンツの再生処理を実行するコンテンツ再生機器であり、コンテンツの配信管理を行なうユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理により生成される前記コンテンツ再生機器の格納鍵により復号可能な暗号化コンテンツ鍵データをショップサーバを介して受信し、該受信する暗号化コンテンツ鍵データに含まれるショップサーバおよびユーザ機器認証サーバ（ＤＡＳ）の署名検証を実行し、データ改竄の無いことが確認されたことを条件として、受信した暗号化コンテンツ鍵データから暗号化コンテンツ鍵を取り出し復号しコンテンツ鍵の取得処理を実行する構成を有することを特徴とするコンテンツ再生機器にある。

【００２８】さらに、本発明の第５の側面は、ユーザ機器（ＤＥＶ）からショップサーバ（ＳＨＯＰ）に対してコンテンツ購入要求を送信するステップと、ショップサーバ（ＳＨＯＰ）において、前記ユーザ機器からのコンテンツ購入要求を受信するステップと、ユーザ機器認証サーバ（ＤＡＳ）において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵から、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵へ変換する鍵かけかえ処理を実行するステップと、前記ショップサーバにおいて前記ユーザ機器によるコンテンツ購入に基づく課金処理が完了したことを条件として、前記ユーザ機器認証サーバの生成したユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバから前記ユーザ機器に提供するステップと、を有することを特徴とするコンテンツ配信方法にある。

【００２９】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵は、前記ユーザ機器認証サーバ（ＤＡＳ）の公開鍵ＫｐＤＡＳで暗号化された暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）であり、前記ユーザ機器認証サーバ（ＤＡＳ）の実行する鍵かけかえ処理は、前記暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を前記ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵ＫｓＤＡＳで復号しコンテンツ鍵Ｋｃを取得し、さらに前記ユーザ機器（ＤＥＶ）の公開鍵ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を生成する処理であることを特徴とする。

【００３０】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器から、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００３１】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器認証サーバは、前記ショップサーバから、前記ユーザ機器の格納鍵では復号不可能な暗号化コンテンツ鍵を受信し、鍵かけかえ処理により生成されるユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ショップサーバに送信し、前記ショップサーバは、前記課金処理の完了を条件として、前記ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を前記ユーザ機器に送信する処理を実行する構成を有することを特徴とする。

【００３２】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器が生成し、前記ショップサーバに対して送信するコンテンツ購入要求データは、要求データ送信先であるショップの識別子としてのショップＩＤ、コンテンツ取り引き識別子としてのトランザクションＩＤ、購入要求対象のコンテンツ識別子としてのコンテンツＩＤを有するとともにユーザ機器の電子署名を含むデータとして構成され、前記ショップサーバは、前記コンテンツ購入要求データの署名検証を実行することによりデータ改竄有無をチェックするとともに、該コンテンツ購入要求データに基づいて、ショップ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ショップでの処理シーケンス遷移を前記ステータス情報に基づいて管理することを特徴とする。

【００３３】さらに、本発明のコンテンツ配信方法の一実施態様において、前記ユーザ機器認証サーバは、前記ユーザ機器または前記ショップサーバのいずれかからの鍵かけかえ要求の受信に応じて、ユーザ機器認証サーバ管理データベースに新規エントリを追加し、該追加エントリに対する処理状況を示すステータス情報を設定し、該ユーザ機器認証サーバでの処理シーケンス遷移を前記ステータス情報に基づいて管理することを特徴とする。

【００３４】さらに、本発明の第６の側面は、コンテンツ鍵の配信処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムを提供するプログラム提供媒体であって、前記コンピュータ・プログラムは、コンテンツ配信を管理するユーザ機器認証サーバ（ＤＡＳ）の生成するユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を受信するステップと、前記ユーザ機器からのコンテンツ購入要求に基づく課金処理を実行するステップと、前記課金処理の完了を条件として、前記ユーザ機器に対して、ユーザ機器の格納鍵により復号可能な暗号化コンテンツ鍵を送信するステップと、を有することを特徴とするプログラム提供媒体にある。

【００３５】なお、本発明の第６の側面に係るプログラム提供媒体は、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ・プログラムをコンピュータ可読な形式で提供する媒体である。媒体は、ＣＤやＦＤ、ＭＯなどの記録媒体、あるいは、ネットワークなどの伝送媒体など、その形態は特に限定されない。

【００３６】このようなプログラム提供媒体は、コンピュータ・システム上で所定のコンピュータ・プログラムの機能を実現するための、コンピュータ・プログラムと提供媒体との構造上又は機能上の協働的関係を定義したものである。換言すれば、該提供媒体を介してコンピュータ・プログラムをコンピュータ・システムにインストールすることによって、コンピュータ・システム上では協働的作用が発揮され、本発明の他の側面と同様の作用効果を得ることができるのである。

【００３７】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。

【００３８】

【発明の実施の形態】以下、図面を参照しながら、本発明の実施の形態について詳細に説明する。なお、説明は、以下の項目に従って行なう。

１．暗号化コンテンツ鍵の鍵かけかえ処理によるコンテンツ配信管理

１．１．システム構成：基本コンテンツ配信モデル１

１．２．基本コンテンツ配信モデル１の変形例

１．３．基本コンテンツ配信モデル２

２．電子チケットを利用したコンテンツ配信モデル

３．ログ収集サーバによるコンテンツ配信管理

４．属性データを記録した公開鍵証明書または属性証明書利用構成

【００３９】

【実施例】［１．暗号化コンテンツ鍵の鍵かけかえ処理によるコンテンツ配信管理］

［１．１．システム構成：基本コンテンツ配信モデル１］図１に本発明のコンテンツ配信システムおよびコンテンツ配信方法の一実施例の概要を説明する図を示す。なお、システムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００４０】図１のコンテンツ配信システムは、ユーザ機器に対するコンテンツの配信サービスを行なうショップサーバ（ＳＨＯＰ）１００、ショップサーバ１００からのコンテンツ配信を受信するユーザ機器（ＤＥＶＩＣＥ）２００、さらに、正当なコンテンツ取り引き管理を行なう管理サーバとして機能するユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）３００を主構成要素とする。なお、図１の構成では、ショップサーバ１００、ユーザ機器２００、ユーザ機器認証サーバ３００を１つづつ示しているが、実際のコンテンツ取り引き構成においては、図１に示す各構成要素が複数存在し、各コンテンツ取り引き毎に、様々なルートで情報が送受信される。図１は、１つのコンテンツ取り引きにおけるデータの流れを示しているものである。

【００４１】（ショップサーバ）図１のコンテンツ配信システムのショップサーバ１００の構成を図２に示す。ショップサーバ１００は、取り引き対象となるコンテンツをコンテンツキーで暗号化した暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）と、コンテンツキーＫｃをユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）の公開鍵：ＫｐＤＡＳで暗号化した暗号化コンテンツキーＫｐＤＡＳ（Ｋｃ）を格納したコンテンツデータベース１１０を有する。なお、暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）は、図にも示すように、それぞれコンテンツ識別子であるコンテンツＩＤが付加され、コンテンツＩＤに基づいて識別可能な構成を持つ。

【００４２】ショップサーバ１００は、さらにコンテンツ取り引き管理データ、例えばコンテンツ販売先のユーザ機器の識別子とコンテンツ識別子等を対応づけて管理する購買管理データベース１２０を有する。さらに、コンテンツデータベース１１０からの配信コンテンツの抽出処理、取り引きに伴う購買管理データベース１２０に対して登録する取り引きデータの生成処理、ユーザ機器２００、ユーザ機器認証サーバ３００との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段１３０を有する。

【００４３】購買管理データベース１２０のデータ構成を図３に示す。購買管理データベース１２０は、ショップサーバがコンテンツ取り引きに応じて処理を実行する際に内部生成する識別番号としてのショップ処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、ユーザ機器とショップ間でのコンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、ショップサーバにおけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【００４４】制御手段１３０は、図２に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段１３０は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段１３０の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ショップサーバ１００が格納する暗号鍵等の暗号処理用データとしては、ショップサーバの秘密鍵：ＫｓＳＨＯＰ、ショップサーバの公開鍵証明書Ｃｅｒｔ＿ＳＨＯＰ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【００４５】図４に制御手段１３０の構成例を示す。制御手段１３０の構成について説明する。制御部１３１は各種処理プログラムを実行する中央演算処理装置（ＣＰＵ:Central Processing Unit）によって構成され、図４の制御手段の各構成部位の処理を制御する。ＲＯＭ（Read only Memory）１３２は、ＩＰＬ（Initial Program Loading）等のプログラムを記憶したメモリである。ＲＡＭ（Random Access Memory）１３３は、制御部１３１が実行するプログラム、例えばデータベース管理プログラム、暗号処理プログラム、通信プログラム等、実行プログラムの格納領域、またこれら各プログラム処理におけるワークエリアとして使用される。

【００４６】表示部１３４は、液晶表示装置、ＣＲＴなどの表示手段を有し、制御部１３１の制御の下、様々なプログラム実行時のデータ、例えばコンテンツ配信先のユーザデータ等を表示する。入力部１３５は、キーボードや、例えばマウス等のポインティングデバイスを有し、これら各入力デバイスからのコマンド、データ入力を制御部１３１に出力する。ＨＤＤ（Hard Disk Drive）１３６は、データベース管理プログラム、暗号処理プログラム、通信プログラム等のプログラム、さらに各種データが格納される。

【００４７】ドライブ１３７は、例えばＨＤ（Hard Disk）や、ＦＤ（Floppy Disk）等の磁気ディスク、ＣＤ－ＲＯＭ（Compact Disk ROM）などの光ディスク、ミニディスク等の光磁気ディスク、ＲＯＭやフラッシュメモリなどの半導体メモリ等の各種記録媒体に対するアクセスを制御する機能を持つ。磁気ディスク等の各種記録媒体はプログラム、データ等を記憶する。ネットワークイン

タフェース１３８は、インターネット、電話回線等の有線、無線を介した通信のインタフェースとして機能する。

【００４８】ショップサーバ１００は、例えば上述した構成を持つ制御手段１３０において、コンテンツの取り引き対象であるユーザ機器２００、あるいはユーザ機器認証サーバ３００との間でのコンテンツ取り引きに伴う様々な暗号処理、認証処理等を実行する。

【００４９】（ユーザ機器認証サーバ）図５にユーザ機器認証サーバ（ＤＡＳ）３００の構成を示す。ユーザ機器認証サーバは、ライセンス管理データベース３２０を有する。ライセンス管理データベース３２０のデータ構成を図６に示す。ライセンス管理データベースは、コンテンツ取り引き時にユーザ機器認証サーバ（ＤＡＳ）の実行する処理に応じて内部生成する処理識別子としてのユーザ機器認証サーバ処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きを実行するショップサーバの識別子であるショップＩＤ、ショップの発行するショップでの処理識別子であるショップ処理Ｎｏ．、ユーザ機器認証サーバ（ＤＡＳ）におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される

【００５０】ユーザ機器認証サーバ（ＤＡＳ）３００は、ユーザ機器２００、ショップサーバ１００との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段３３０を有する。制御手段３３０は、先に説明したショップサーバの制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図４を用いて説明した構成と同様である。制御手段３３０の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ユーザ機器認証サーバ（ＤＡＳ）３００が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵：ＫｓＤＡＳ、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵証明書Ｃｅｒｔ＿ＤＡＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【００５１】（ユーザ機器）図７にユーザ機器２００の構成を示す。ユーザ機器は、コンテンツの購入を実行し、購入したコンテンツの利用、すなわちコンテンツ再生、実行を行なう例えばコンテンツ再生機器であり、購入管理データベース２２０を有する。購入管理データベース２２０のデータ構成を図８に示す。購入管理データベースは、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するコンテンツ取り引き識別子としてのトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きを実行するショップサーバの識別子であるショップＩＤ、ユーザ機器におけるコンテンツ取り引き処理のステータスを示すステータスの各情報、さらに、ユーザ機器の機器識別子である機器ＩＤを持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【００５２】ユーザ機器２００は、ショップサーバ１００、ユーザ機器認証サーバ３００との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段２３０を有する。制御手段２３０は、先に説明したショップサーバの制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図４を用いて説明した構成と同様である。制御手段２３０の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ユーザ機器２００が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器の秘密鍵：ＫｓＤＥＶ、ユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡ、コンテンツをユーザ機器の例えばハードディスク等の記憶手段に格納する際の暗号化鍵として適用する保存鍵Ｋｓｔｏがある。

【００５３】［公開鍵証明書］上記ショップサーバ（ＳＨＯＰ）１００、ユーザ機器（ＤＥＶＩＣＥ）２００、ユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）３００の保有する公開鍵証明書について図９を用いて説明する。

【００５４】公開鍵証明書は、公開鍵を用いた暗号データの送受信、あるいはデータ送受信を行なう２者間での相互認証等の処理において、使用する公開鍵が正当な利用者の有する公開鍵であることを第三者、すなわち発行局（ＣＡ：Certificate Authority）が証明したものである。公開鍵証明書のフォーマットの概略を図９（ａ）に示す。

【００５５】バージョン（version）は、証明書フォーマットのバージョンを示す。証明書の通し番号は、シリアルナンバ（Serial Number）であり、公開鍵証明書発行局（ＣＡ）によって設定される公開鍵証明書のシリアルナンバである。署名アルゴリズム識別子、アルゴリズムパラメータ（Signature algorithm Identifier algorithm parameter）は、公開鍵証明書の署名アルゴリズムとそのパラメータを記録するフィールドである。なお、署名アルゴリズムとしては、楕円曲線暗号およびＲＳＡがあり、楕円曲線暗号が適用されている場合はパラメータおよび鍵長が記録され、ＲＳＡが適用されている場合には鍵長が記録される。発行局の名前は、公開鍵証明書

の発行者、すなわち公開鍵証明書発行局（ＣＡ）の名称が識別可能な形式（Distinguished Name）で記録されるフィールドである。証明書の有効期限(validity)は、証明書の有効期限である開始日時、終了日時が記録される。公開鍵証明書の利用者名（ＩＤ）は、ユーザである認証対象者の名前が記録される。具体的には例えばユーザ機器のＩＤや、サービス提供主体のＩＤ等である。利用者公開鍵（subject Public Key Info algorithm subject Public key）は、ユーザの公開鍵情報としての鍵アルゴリズム、鍵情報そのものを格納するフィールドである。発行局が付ける署名は、公開鍵証明書発行局（ＣＡ）の秘密鍵を用いて公開鍵証明書のデータに対して実行される電子署名であり、公開鍵証明書の利用者は、公開鍵証明書発行局（ＣＡ）の公開鍵を用いて検証を行ない、公開鍵証明書の改竄有無がチェック可能となっている。

【００５６】公開鍵暗号方式を用いた電子署名の生成方法について、図１０を用いて説明する。図１０に示す処理は、ＥＣ－ＤＳＡ（（Elliptic Curve Digital SignatureAlgorithm）、IEEE P1363/D3）を用いた電子署名データの生成処理フローである。なお、ここでは公開鍵暗号として楕円曲線暗号（Elliptic Curve Cryptography（以下、ＥＣＣと呼ぶ））を用いた例を説明する。なお、本発明のデータ処理装置においては、楕円曲線暗号以外にも、同様の公開鍵暗号方式における、例えばＲＳＡ暗号（（Rivest、Shamir、Adleman）など（ANSI X9.31））を用いることも可能である。

【００５７】図１０の各ステップについて説明する。ステップＳ１において、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$4a^3+27b^2\neq 0$（ｍｏｄ　ｐ）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、Ｋｓを秘密鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ２おいて、メッセージMのハッシュ値を計算し、f=Hash(M)とする。

【００５８】ここで、ハッシュ関数を用いてハッシュ値を求める方法を説明する。ハッシュ関数とは、メッセージを入力とし、これを所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの1ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ異なる入力データを探し出すことが困難である特徴を有する。ハッシュ関数としては、ＭＤ４、ＭＤ５、ＳＨＡ－１などが用いられる場合もあるし、ＤＥＳ－ＣＢＣが用いられる場合もある。この場合は、最終出力値となるＭＡＣ（チェック値：ＩＣＶに相当する）がハッシュ値となる。

【００５９】続けて、ステップＳ３で、乱数ｕ（０＜ｕ＜ｒ）を生成し、ステップＳ４でベースポイントをｕ倍した座標Ｖ（Ｘｖ，Ｙｖ）を計算する。なお、楕円曲線上の加算、２倍算は次のように定義されている。

【００６０】

【数１】P=(Ｘａ，Ｙａ),Q=(Ｘｂ，Ｙｂ),R=(Ｘｃ,Ｙｃ)=P+Qとすると、P≠Qの時（加算）、

$Xc=\lambda^2-Xa-Xb$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(Yb-Ya)/(Xb-Xa)$

P=Qの時（2倍算）、

$Xc=\lambda^2-2Xa$

$Yc=\lambda\times(Xa-Xc)-Ya$

$\lambda=(3(Xa)^2+a)/(2Ya)$

【００６１】これらを用いて点Ｇのｕ倍を計算する（速度は遅いが、最もわかりやすい演算方法として次のように行う。Ｇ、２×Ｇ、４×Ｇ・・を計算し、uを2進数展開して1が立っているところに対応する$2^i\times G$（Ｇをｉ回２倍算した値（ｉはｕのＬＳＢから数えた時のビット位置））を加算する。

【００６２】ステップＳ５で、ｃ＝Ｘｖｍｏｄ　ｒを計算し、ステップＳ６でこの値が０になるかどうか判定し、０でなければステップＳ７でｄ＝［（ｆ＋ｃＫｓ）／ｕ］ｍｏｄ　ｒを計算し、ステップＳ８でｄが０であるかどうか判定し、ｄが０でなければ、ステップＳ９でｃおよびｄを電子署名データとして出力する。仮に、ｒを１６０ビット長の長さであると仮定すると、電子署名データは３２０ビット長となる。

【００６３】ステップＳ６において、ｃが０であった場合、ステップＳ３に戻って新たな乱数を生成し直す。同様に、ステップＳ８でｄが０であった場合も、ステップＳ３に戻って乱数を生成し直す。

【００６４】次に、公開鍵暗号方式を用いた電子署名の検証方法を、図１１を用いて説明する。ステップＳ１１で、Ｍをメッセージ、ｐを標数、a、bを楕円曲線の係数（楕円曲線：$y^2=x^3+ax+b$）、Ｇを楕円曲線上のベースポイント、ｒをＧの位数、ＧおよびＫｓ×Ｇを公開鍵（０＜Ｋｓ＜ｒ）とする。ステップＳ１２で電子署名データｃおよびｄが０＜ｃ＜ｒ、０＜ｄ＜ｒを満たすか検証する。これを満たしていた場合、ステップＳ１３で、メッセージMのハッシュ値を計算し、ｆ＝Ｈａｓｈ（Ｍ）とする。次に、ステップＳ１４でh=1/d mod rを計算し、ステップＳ１５でｈ１＝ｆｈ　ｍｏｄ　ｒ、ｈ２=ｃｈ　ｍｏｄ　ｒを計算する。

【００６５】ステップＳ１６において、既に計算したｈ１およびｈ２を用い、点Ｐ＝（Ｘｐ，Ｙｐ）＝ｈ１×Ｇ＋ｈ２・Ｋｓ×Ｇを計算する。電子署名検証者は、公開鍵ＧおよびＫｓ×Ｇを知っているので、図１０のステップＳ４と同様に楕円曲線上の点のスカラー倍の計算ができる。そして、ステップＳ１７で点Ｐが無限遠点かどうか判定し、無限遠点でなければステップＳ１８に進む（実際には、無限遠点の判定はステップＳ１６でできてしまう。つまり、Ｐ＝（Ｘ，Ｙ）、Ｑ＝（Ｘ，－Ｙ）の加算を行うと、λが計算できず、Ｐ＋Ｑが無限遠点であ

ることが判明している）。ステップＳ１８でＸｐ ｍｏｄ ｒを計算し、電子署名データｃと比較する。最後に、この値が一致していた場合、ステップＳ１９に進み、電子署名が正しいと判定する。

【００６６】電子署名が正しいと判定された場合、データは改竄されておらず、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したことがわかる。

【００６７】ステップＳ１２において、電子署名データｃまたはｄが、０＜ｃ＜ｒ、０＜ｄ＜ｒを満たさなかった場合、ステップＳ２０に進む。また、ステップＳ１７において、点Ｐが無限遠点であった場合もステップＳ２０に進む。さらにまた、ステップＳ１８において、Ｘｐ ｍｏｄ ｒの値が、電子署名データｃと一致していなかった場合にもステップＳ２０に進む。

【００６８】ステップＳ２０において、電子署名が正しくないと判定された場合、データは改竄されているか、公開鍵に対応した秘密鍵を保持する者が電子署名を生成したのではないことがわかる。

【００６９】公開鍵証明書には、発行局の署名がなされ、公開鍵利用者による署名検証により、証明書の改竄がチェック可能な構成となっている。図９に戻り説明をつづける。図９（ｂ）がユーザ機器に格納されるユーザ機器の公開鍵証明書：Ｃｅｒｔ＿ＤＥＶであり、ユーザ機器ＩＤと、ユーザ機器の公開鍵ＫｐＤＥＶを格納している。図９（ｃ）はショップサーバに格納されるショップサーバの公開鍵証明書：Ｃｅｒｔ＿ＳＨＯＰであり、ショップＩＤと、ショップサーバの公開鍵ＫｐＳＨＯＰを格納している。図９（ｄ）はユーザ機器認証サーバに格納されるユーザ機器認証サーバの公開鍵証明書：Ｃｅｒｔ＿ＤＡＳであり、ユーザ機器認証サーバＩＤと、ユーザ機器認証サーバの公開鍵ＫｐＤＡＳを格納している。このように、ユーザ機器、ショップサーバ、ユーザ機器認証サーバがそれぞれ公開鍵証明書を保有する。

【００７０】［コンテンツ購入処理］次に、図１に戻り、ユーザ機器が、ショップサーバからコンテンツを購入して利用する処理について説明する。図１の番号（１）から（２０）の順に処理が進行する。各番号順に処理の詳細を説明する。なお、本実施例ではエンティティ間の通信において相互認証処理（（１）、（７）、（１１））を行なったものを述べているが、必要に応じて省略しても構わない。

【００７１】（１）相互認証

コンテンツをショップサーバ１００から購入しようとするユーザ機器２００は、ショップサーバとの間で相互認証処理を行なう。データ送受信を実行する２つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。

【００７２】共通鍵暗号方式を用いた相互認証方法を、図１２を用いて説明する。図１２において、共通鍵暗号方式としてＤＥＳを用いているが、同様な共通鍵暗号方式であればいずれでもよい。

【００７３】まず、Ｂが６４ビットの乱数Ｒｂを生成し、Ｒｂおよび自己のＩＤであるＩＤ（ｂ）をＡに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａを生成し、Ｒａ、Ｒｂ、ＩＤ（ｂ）の順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いてデータを暗号化し、Ｂに返送する。

【００７４】これを受信したＢは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、まず、暗号文Ｅ１を鍵Ｋａｂで復号化し、乱数Ｒａを得る。次に、暗号文Ｅ２を鍵Ｋａｂで復号化し、その結果とＥ１を排他的論理和し、Ｒｂを得る。最後に、暗号文Ｅ３を鍵Ｋａｂで復号化し、その結果とＥ２を排他的論理和し、ＩＤ(ｂ)を得る。こうして得られたＲａ、Ｒｂ、ＩＤ(ｂ)の内、ＲｂおよびＩＤ(ｂ)が、Ｂが送信したものと一致するか検証する。この検証に通った場合、ＢはＡを正当なものとして認証する。

【００７５】次にＢは、認証後に使用するセッション鍵（Session Key（以下、Ｋｓｅｓとする））を生成する（生成方法は、乱数を用いる）。そして、Ｒｂ、Ｒａ、Ｋｓｅｓの順に、ＤＥＳのＣＢＣモードで鍵Ｋａｂを用いて暗号化し、Ａに返送する。

【００７６】これを受信したＡは、受信データを鍵Ｋａｂで復号化する。受信データの復号化方法は、Ｂの復号化処理と同様であるので、ここでは詳細を省略する。こうして得られたＲｂ、Ｒａ、Ｋｓｅｓの内、ＲｂおよびＲａが、Ａが送信したものと一致するか検証する。この検証に通った場合、ＡはＢを正当なものとして認証する。互いに相手を認証した後には、セッション鍵Ｋｓｅｓは、認証後の秘密通信のための共通鍵として利用される。

【００７７】なお、受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【００７８】次に、公開鍵暗号方式である１６０ビット長の楕円曲線暗号を用いた相互認証方法を、図１３を用いて説明する。図１３において、公開鍵暗号方式としてＥＣＣを用いているが、前述のように同様な公開鍵暗号方式であればいずれでもよい。また、鍵サイズも１６０ビットでなくてもよい。図１３において、まずＢが、６４ビットの乱数Ｒｂを生成し、Ａに送信する。これを受信したＡは、新たに６４ビットの乱数Ｒａおよび標数ｐより小さい乱数Ａｋを生成する。そして、ベースポイントＧをＡｋ倍した点Ａｖ＝Ａｋ×Ｇを求め、Ｒａ、Ｒｂ、Ａｖ（X座標とY座標）に対する電子署名Ａ．Ｓｉｇ

を生成し、Ａの公開鍵証明書とともにＢに返送する。ここで、ＲａおよびＲｂはそれぞれ６４ビット、ＡｖのＸ座標とＹ座標がそれぞれ１６０ビットであるので、合計４４８ビットに対する電子署名を生成する。

【００７９】公開鍵証明書を利用する際には、利用者は自己が保持する公開鍵証明書発行局（ＣＡ）４１０の公開鍵を用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局（ＣＡ）の公開鍵を保持している必要がある。なお、電子署名の検証方法については、図１１で説明したのでその詳細は省略する。

【００８０】Ａの公開鍵証明書、Ｒａ、Ｒｂ、Ａｖ、電子署名Ａ．Ｓｉｇを受信したＢは、Ａが送信してきたＲｂが、Ｂが生成したものと一致するか検証する。その結果、一致していた場合には、Ａの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ａの公開鍵を取り出す。そして、取り出したＡの公開鍵を用い電子署名Ａ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＢはＡを正当なものとして認証する。

【００８１】次に、Ｂは、標数ｐより小さい乱数Ｂｋを生成する。そして、ベースポイントＧをＢｋ倍した点Ｂｖ＝Ｂｋ×Ｇを求め、Ｒｂ、Ｒａ、Ｂｖ（Ｘ座標とＹ座標）に対する電子署名Ｂ．Ｓｉｇを生成し、Ｂの公開鍵証明書とともにＡに返送する。

【００８２】Ｂの公開鍵証明書、Ｒｂ、Ｒａ、Ｂｖ、電子署名Ｂ．Ｓｉｇを受信したＡは、Ｂが送信してきたＲａが、Ａが生成したものと一致するか検証する。その結果、一致していた場合には、Ｂの公開鍵証明書内の電子署名を認証局の公開鍵で検証し、Ｂの公開鍵を取り出す。そして、取り出したＢの公開鍵を用い電子署名Ｂ．Ｓｉｇを検証する。電子署名の検証に成功した後、ＡはＢを正当なものとして認証する。

【００８３】両者が認証に成功した場合には、ＢはＢｋ×Ａｖ（Ｂｋは乱数だが、Ａｖは楕円曲線上の点であるため、楕円曲線上の点のスカラー倍計算が必要）を計算し、ＡはＡｋ×Ｂｖを計算し、これら点のＸ座標の下位６４ビットをセッション鍵として以降の通信に使用する（共通鍵暗号を６４ビット鍵長の共通鍵暗号とした場合）。もちろん、Ｙ座標からセッション鍵を生成してもよいし、下位６４ビットでなくてもよい。なお、相互認証後の秘密通信においては、送信データはセッション鍵で暗号化されるだけでなく、電子署名も付されることがある。

【００８４】電子署名の検証や受信データの検証の際に、不正、不一致が見つかった場合には、相互認証が失敗したものとして処理を中断する。

【００８５】このような相互認証処理において、生成したセッション鍵を用いて、送信データを暗号化して、相互にデータ通信を実行する。

【００８６】（２）トランザクションＩＤ、購入要求データ生成、および

（３）購入要求データ送信

上述のショップサーバ１００とユーザ機器２００間の相互認証が成功すると、ユーザ機器２００は、コンテンツの購入要求データを生成する。購入要求データの構成を図１４（ａ）に示す。購入要求データは、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、コンテンツ取り引きの識別子として、ユーザ機器２００の暗号処理手段が例えば乱数に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ショップ側に送付済みの場合は、必ずしも改めて送付する必要はない。

【００８７】（４）受信データ検証

図１４（ａ）に示す購入要求データをユーザ機器２００から受信したショップサーバ１００は、受信データの検証処理を実行する。検証処理の詳細について図１５を用いて説明する。まず、ショップサーバ１００は、受信データ中のユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶの検証（Ｓ５１）を行なう。これは前述したように、公開鍵証明書に含まれる発行局（ＣＡ）の署名を検証する処理（図１１参照）として実行され、発行局の公開鍵：ＫｐＣＡを適用して実行される。

【００８８】検証がＯＫ、すなわち公開鍵証明書の改竄がないと判定（Ｓ５２でＹｅｓ）されると、Ｓ５３に進む。検証が非成立の場合（Ｓ５２でＮｏ）は、Ｓ５７で公開鍵証明書に改竄ありと判定され、その公開鍵証明書を利用した処理が中止される。Ｓ５３では、公開鍵証明書からユーザ機器の公開鍵：ＫｐＤＥＶが取り出され、ステップＳ５４で公開鍵：ＫｐＤＥＶを用いた購入要求データのユーザ機器署名の検証処理（図１１参照）が実行される。検証がＯＫ、すなわち購入要求データの改竄がないと判定（Ｓ５５でＹｅｓ）されると、Ｓ５６に進み受信データが正当なコンテンツ購入要求データであると判定される。検証が非成立の場合（Ｓ５５でＮｏ）は、Ｓ５７で購入要求データが改竄ありと判定され、その購入要求データに対する処理が中止される。

【００８９】（５）暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショップ）送信

ショップサーバ１００において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ１００は、暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショッ

プ）をユーザ機器に送信する。これらは、いずれもコンテンツデータベース１１０に格納されたデータであり、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Ｋｃ（content）と、コンテンツキー：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵で暗号化した暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）である。

【００９０】暗号化コンテンツ鍵データ１（ショップ）の構成を図１４（ｂ）に示す。暗号化コンテンツ鍵データ１（ショップ）は、コンテンツ購入の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、購入要求データ（図１４（ａ）のユーザ機器公開鍵証明書を除いたデータ）、コンテンツ取り引きに伴いショップサーバ１００が生成したショップ処理Ｎｏ．、暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ１（ショップ）には、ショップサーバ１００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【００９１】（６）受信データ検証

ショップサーバ１００から暗号化コンテンツ：Ｋｃ（content）と、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を受信したユーザ機器２００は、暗号化コンテンツ鍵データ１（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）のショップ署名の検証を実行する。

【００９２】（７）相互認証

ユーザ機器２００が、ショップサーバ１００から暗号化コンテンツ：Ｋｃ（content）と暗号化コンテンツ鍵データ１（ショップ）を受信し、暗号化コンテンツ鍵データ１（ショップ）の検証を終えると、ユーザ機器２００は、ユーザ機器認証サーバ３００にアクセスし、ユーザ機器２００と、ユーザ機器認証サーバ３００間において相互認証処理を実行する。この処理は、前述のショップサーバ１００とユーザ機器２００間の相互認証処理と同様の手続きで実行される。

【００９３】（８）暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求送信

ユーザ機器２００とユーザ機器認証サーバ３００との間の相互認証が成立すると、ユーザ機器２００は、ユーザ機器認証サーバ３００に対して、先にショップサーバ１００から受信した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を含む暗号化コンテンツ鍵データ（ユーザ機器）と、暗号化コンテンツ鍵かけかえ要求を送信する。

【００９４】暗号化コンテンツ鍵データ（ユーザ機器）の構成を図１４（ｃ）に示す。暗号化コンテンツ鍵データ（ユーザ機器）は、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ３００の識別子であるユーザ機器認証サーバＩＤ、ショップサーバ１００から受領した暗号化コンテンツ鍵データ（図１４（ｂ）のショップ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するユーザ機器２００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ユーザ機器）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器２００の公開鍵証明書が添付され、ユーザ機器認証サーバ３００に送付される。なお、ユーザ機器認証サーバ３００がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【００９５】（９）受信データ検証

ユーザ機器２００から暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求（図１４（ｃ））を受信したユーザ機器認証サーバ３００は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器認証サーバ３００は、まずユーザ機器２００から受領したユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて、図１４（ａ）に示す購入要求データおよび図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）の電子署名の検証を実行する。さらに、ショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）に含まれる（５）暗号化コンテンツ鍵データ１のショップ署名の検証を実行する。

【００９６】（１０）暗号化コンテンツ鍵かけかえ処理、ユーザ機器認証サーバ３００において、ユーザ機器２００から受信した暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求の検証が終了し、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ（ユーザ機器）に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ３００の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋ

ｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。

【００９７】図１６にユーザ機器認証サーバ３００において実行される暗号化コンテンツ鍵かけかえ処理のフローを示す。まず、ユーザ機器認証サーバ３００は、ユーザ機器２００から受信した暗号化コンテンツ鍵データ（ユーザ機器）から、ユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を取り出す（Ｓ６１）。次に、ユーザ機器認証サーバ３００の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得（Ｓ６２）する。次に、復号により取得したコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する（Ｓ６３）。これらの処理が終了すると、ライセンス管理データベース（図６参照）のステータスを「鍵かけかえ完了」に設定する。

【００９８】（１１）相互認証

ユーザ機器認証サーバ３００において、上述の暗号化コンテンツ鍵の鍵かけかえ処理が完了すると、ユーザ機器認証サーバ３００は、ショップサーバ１００にアクセスし、ユーザ機器認証サーバ３００とショップサーバ１００間において相互認証処理を実行する。この処理は、前述のショップサーバ１００とユーザ機器２００間の相互認証処理と同様の手続きで実行される。

【００９９】（１２）暗号化コンテンツデータ送信

ユーザ機器認証サーバ３００とショップサーバ１００間の相互認証が成立すると、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００に送信する。

【０１００】暗号化コンテンツ鍵データ（ＤＡＳ）の構成を図１７（ｄ）に示す。暗号化コンテンツ鍵データ（ＤＡＳ）は、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、暗号化コンテンツ鍵データ（ユーザ機器）（図１４（ｃ）のショップおよびユーザ機器公開鍵証明書を除いたデータ）、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ３００が生成した暗号化コンテンツ鍵データ：ＫｐＤＥＶ（Ｋｃ）を有し、これらのデータに対するユーザ機器認証サーバ３００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ＤＡＳ）には、ユーザ機器認証サーバ３００と、ユーザ機器２００の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【０１０１】また、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ（ＤＡＳ）は、図１７（ｄ）に示すようにユーザ機器の生成した（８）暗号化コンテンツ鍵データ（ユーザ機器）をそのまま含むデータ構成とすることなく、図１８（ｄ’）に示すように、ユーザ機器ＩＤ、トランザクションＩＤ、コンテンツＩＤ、ショップ処理ＮＯ、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）の各データを、ユーザ機器認証サーバ３００が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ（ＤＡＳ）としてもよい。この場合は、（８）暗号化コンテンツ鍵データ（ユーザ機器）の検証が不要となるので、添付する公開鍵証明書は、ユーザ機器認証サーバ３００の公開鍵証明書のみでよい。

【０１０２】（１３）受信データ検証

ユーザ機器認証サーバ３００から暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ））を受信したショップサーバ１００は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ショップサーバ１００は、まずユーザ機器認証サーバ３００から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）に含まれる（８）暗号化コンテンツ鍵データ（ユーザ機器）のユーザ機器署名の検証を実行する。さらに、また、自己の公開鍵ＫｐＳＨＯＰを用いて、暗号化コンテンツデータ（ユーザ機器）を検証するようにしてもよい。

【０１０３】なお、先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００が受領した場合は、ショップサーバ１００は、ユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図１８（ｄ’）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行するのみの処理となる。

【０１０４】（１４）相互認証、および（１５）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器２００は、暗号化コンテンツ鍵要求データをショップサーバ１００に対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証を実行して、相互認証が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器２００からショップサーバ１００に送信される。

【０１０５】暗号化コンテンツ鍵要求データの構成を図

１７（ｅ）に示す。暗号化コンテンツ鍵要求データは、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、先にユーザ機器２００が生成したコンテンツ取り引きの識別子であるトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤ、さらに、先にショップが生成し暗号化コンテンツ鍵データ１（ショップ）としてユーザ機器２００に送信してきたデータ（図１４（ｂ）参照）中に含まれるショップ処理Ｎｏ．を有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、暗号化コンテンツ鍵要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、公開鍵証明書が既にショップ側に保管済みの場合は、必ずしも改めて送付する必要はない。

【０１０６】（１６）検証処理、および
（１７）課金処理
暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１００は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図１５を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ１００は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【０１０７】この課金処理に至るまでには、ユーザ機器認証サーバ３００による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ１００は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器２００においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【０１０８】（１８）暗号化コンテンツ鍵データ２（ショップ）送信
ショップサーバ１００における課金処理が終了すると、ショップサーバ１００は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器２００に送信する。

【０１０９】暗号化コンテンツ鍵データ２（ショップ）の構成を図１７（ｆ）に示す。暗号化コンテンツ鍵データ２（ショップ）は、暗号化コンテンツ鍵要求の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、ユーザ機器認証サーバ３００から受領した暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）のユーザ機器、ユーザ機器認証サーバ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ２（ショップ）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ユーザ機器２００がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０１１０】なお、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在であり、ショップサーバ１００がユーザ機器認証サーバ３００から受信する暗号化コンテンツ鍵データ（ＤＡＳ）が先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）である場合は、ショップサーバ１００は、図１８（ｆ’）に示す暗号化コンテンツ鍵データ２（ショップ）をユーザ機器に送付する。すなわち、図１８（ｄ’）に示す簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）にショップサーバの署名を付加したデータに、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書を添付してユーザ機器２００に送付する。

【０１１１】（１９）受信データ検証
ショップサーバ１００から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバ１００の公開鍵ＫｐＳＨＯＰを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ３００の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）に含まれる（１２）暗号化コンテンツ鍵データ（ＤＡＳ）の署名検証を実行する。さらにまた、自己の公開鍵ＫｐＤＥＶを用いて、暗号化コンテンツデータ（ユーザ機器）を検証するようにしてもよい。

【０１１２】（２０）保存処理
ショップサーバ１００から受信した暗号化コンテンツ鍵データ２（ショップ）を検証したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）に含まれる自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用

いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器２００の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０１１３】ユーザ機器２００におけるコンテンツ鍵Ｋｃの取得と保存処理フローを図１９に示す。ユーザ機器２００は、まず、ショップサーバ１００から受信した暗号化コンテンツ鍵データ２（ショップ）から自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を取り出し（Ｓ７１）、取り出した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号してコンテンツ鍵Ｋｃを取り出す（Ｓ７２）。さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いてコンテンツ鍵Ｋｃの暗号化処理を実行して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器２００の記憶手段（内部メモリ）に格納（Ｓ７３）する。

【０１１４】以上の処理により、ユーザ機器は、暗号化コンテンツＫｃ（Content）と、該暗号化コンテンツのコンテンツ鍵Ｋｃを取得することができ、コンテンツを利用することができる。上述の説明から明らかなように、ユーザ機器２００においてコンテンツ利用可能な状態に至るまでには、ユーザ機器認証サーバ３００における暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須である。従って、ショップサーバ１００は、ユーザ機器２００に対して、ユーザ機器認証サーバ３００に秘密にコンテンツを販売し、コンテンツをユーザ機器において利用可能な状態とすることができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべてのショップの取り引きの管理がなされ、課金されたコンテンツ取り引きを把握し、ショップの課金処理において受領されたコンテンツ料金を、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に正確に配分することが可能となる。

【０１１５】（各機器におけるステータス遷移）図１に示すショップサーバ１００、ユーザ機器２００、ユーザ認証サーバ（ＤＡＳ）３００は、それぞれコンテンツ取り引きに係る一連の処理において、処理状態を示すステータスに応じて、次の処理を決定する。ステータスは、例えば図３に示すショップサーバの購買管理データベース、図６のユーザ機器認証サーバのライセンス管理データベース、図８のユーザ機器の購入管理データベースにおいて、各コンテンツ取り引き毎に管理される。

【０１１６】まず、ショップサーバ１００のステータス遷移について、図２０を用いて説明する。ショップサーバは、ユーザ機器２００からのコンテンツ購入要求データを受信（図１の処理（３）に対応）することで処理が開始される。ショップサーバ１００は、ユーザ機器２００からの受信データを検証し、検証に成功した場合は、ステータスを「購入受付完了」に設定し、データ検証により正当な購入要求であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、購入受付処理を所定回数繰り返した後処理を中止し、ステータスを「購入受付失敗」とする。ステータスが「購入受付完了」である場合にのみ次ステップに進む。

【０１１７】ステータスが「購入受付完了」に遷移すると、次に、ショップサーバ１００は、ユーザ機器２００に対して暗号化コンテンツ鍵データ１（ショップ）を送信（図１の処理（５）に対応）し、ユーザ機器からの受信応答（レスポンス）を受領することにより、ステータスを「鍵１配信完了」とする。鍵データ１の送信が成功しなかった場合は、処理を中止するか、あるいは同様の処理、ここでは、鍵データ１の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵１配信失敗」とする。ステータスが「鍵１配信完了」である場合にのみ次ステップに進む。

【０１１８】ステータスが「鍵１配信完了」に遷移した場合、次に、ショップサーバ１００は、ユーザ機器認証サーバ３００から暗号化コンテンツ鍵データ（ＤＡＳ）を受信（図１の処理（１２）に対応）し、データ検証を実行する。検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当な暗号化コンテンツ鍵データ（ＤＡＳ）であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【０１１９】ステータスが「鍵受信完了」に遷移した場合、次に、ショップサーバ１００は、ユーザ機器２００から暗号化コンテンツ鍵送信要求データを受信（図１の処理（１５）に対応）し、データ検証を実行する。検証に成功した場合は、ステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定し、データ検証により正当な鍵送信要求データであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵送信要求データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「暗号化コンテンツ鍵送信要求受付失敗」とする。ステータスが「暗号化コンテンツ鍵送信要求受付完了」である場合にのみ次ステップに進む。

【０１２０】ステータスが「暗号化コンテンツ鍵送信要

求受付完了」に遷移した場合、次に、ショップサーバ１００は、課金処理（図１の処理（１７）に対応）を実行する。課金処理が完了すると、ステータスを「課金完了」に設定し、課金処理が終了しなかった場合、例えばユーザ機器の指定口座からのコンテンツ料金引き落としができなかった場合などには、以降の処理は実行せず、処理を中止するか、あるいは同様の処理、ここでは、課金処理を所定回数繰り返した後、処理を中止し、ステータスを「課金失敗」とする。ステータスが「課金完了」である場合にのみ次ステップに進む。

【０１２１】ステータスが「課金完了」に遷移した場合、次に、ショップサーバ１００は、ユーザ機器へ暗号化コンテンツ鍵データ２（ショップ）送信処理（図１の処理（１８）に対応）を実行する。暗号化コンテンツ鍵データ２（ショップ）送信処理が完了し、ユーザ機器からの受信レスポンスを受信すると、ステータスを「鍵２配信完了」に設定し、鍵データ２（ショップ）送信処理が終了しなかった場合には、ステータスを「鍵２配信失敗」とする。ステータスが「鍵２配信完了」である場合にのみ次ステップ、ここでは処理終了となり、ステータスが「鍵２配信失敗」である場合は、以降の処理は実行せず、処理を中止するか、あるいは同様の処理、ここでは、鍵データ２（ショップ）送信処理を所定回数繰り返す。ショップサーバ１００は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０１２２】次に、ユーザ機器２００のステータス遷移について、図２１を用いて説明する。ユーザ機器２００は、まず、ショップサーバ１００に対してコンテンツ購入要求データを送信（図１の処理（３）に対応）することで処理が開始される。ユーザ機器２００は、ショップサーバ１００に対するコンテンツ購入要求データの受信完了のレスポンスを受信すると、ステータスを「購入要求送信完了」に設定し、ショップサーバ１００からの受信完了のレスポンスを受信できない場合は、処理を中止するか、あるいは同様の処理、ここでは、購入要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「購入要求送信失敗」とする。ステータスが「購入要求送信完了」である場合にのみ次ステップに進む。

【０１２３】ステータスが「購入要求送信完了」に遷移すると、次に、ユーザ機器２００は、ショップサーバ１００から、暗号化コンテンツ鍵データ１（シヨップ）を受信（図１の処理（５）に対応）し、受信データを検証する。ショップサーバ１００からの暗号化コンテンツ鍵データの検証に成功した場合は、ステータスを「鍵１受信完了」に設定し、データ検証により正当な暗号化コンテンツ鍵データであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵１受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵１受信失敗」とする。ステータスが「鍵１受信完了」である場合にのみ次ステップに進む。

【０１２４】ステータスが「鍵１受信完了」に遷移した場合、次に、ユーザ機器２００は、ユーザ機器認証サーバ３００に対して、暗号化コンテンツ鍵データ（ユーザ機器）を送信（図１の処理（８）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、鍵送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。ステータスが「鍵送信完了」である場合にのみ次ステップに進む。

【０１２５】ステータスが「鍵送信完了」に遷移した場合、次に、ユーザ機器２００は、ショップサーバ１００に対して、暗号化コンテンツ鍵送信要求を送信（図１の処理（１５）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵送信要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「暗号化コンテンツ鍵送信要求送信失敗」とする。ステータスが「暗号化コンテンツ鍵送信要求送信完了」である場合にのみ次ステップに進む。

【０１２６】ステータスが「暗号化コンテンツ鍵送信要求送信完了」に遷移した場合、次に、ユーザ機器２００は、ショップサーバ１００から、暗号化コンテンツ鍵データ２（ショップ）を受信（図１の処理（１８）に対応）し、データ検証を行なう。データ検証に成功した場合は、ステータスを「鍵２受信完了」に設定し、データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データ２（ショップ）受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵２受信失敗」とする。ステータスが「鍵２受信完了」である場合には処理終了となる。ユーザ機器２００は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０１２７】次にユーザ機器認証サーバ３００のステータス遷移について、図２２を用いて説明する。ユーザ機器認証サーバ３００は、ユーザ機器２００からの暗号化コンテンツ鍵データ（ユーザ機器）を受信（図１の処理（８）に対応）することで処理が開始される。ユーザ機器認証サーバ３００は、ユーザ機器２００からの受信データを検証し、検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ユーザ機器）の受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失

敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【０１２８】ステータスが「鍵受信完了」に遷移すると、次に、ユーザ機器認証サーバ３００は、コンテンツ鍵かけかえ処理（図１の処理（１０）に対応）を実行し、鍵かけかえ処理が完了した場合には、ステータスを「鍵かけかえ完了」とする。鍵かけかえに失敗することは想定していないので、ここでは「鍵かけかえ完了」のみのステータス遷移が存在する。

【０１２９】ステータスが「鍵かけかえ完了」に遷移した場合、次に、ユーザ機器認証サーバ３００は、ショップサーバ１００に対して暗号化コンテンツ鍵データ（ＤＡＳ）を送信（図１の処理（１２）に対応）し、ショップサーバ１００からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ＤＡＳ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。ステータスが「鍵送信完了」である場合には、処理終了となる。ユーザ機器認証サーバ３００は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０１３０】（コンテンツ購入処理フロー）次に、ユーザ機器からショップサーバに対するコンテンツ購入要求に伴ってショップサーバ１００、ユーザ機器２００、ユーザ機器認証サーバ３００間で実行されるデータ送受信処理をフローに従って説明する。処理フローは、以下のＡ，Ｂ，Ｃ，Ｄに分割して説明する。

【０１３１】Ａ．ショップサーバとユーザ機器間における処理（図１に示す（１）～（６）の処理）

ユーザ機器２００とショップサーバ１００の相互認証～ユーザ機器２００からショップサーバ１００に対するコンテンツ購入要求～ショップサーバ１００からユーザ機器２００に対する鍵１（ショップ）の送信。

Ｂ．ユーザ機器認証サーバとユーザ機器間における処理（図１に示す（７）～（９）の処理）

ユーザ機器２００とユーザ機器認証サーバ３００の相互認証～暗号化コンテンツ鍵データ送信～ユーザ機器認証サーバ３００における受信データ検証。

Ｃ．ユーザ機器認証サーバとショップサーバ間における処理（図１に示す（１１）～（１３）の処理）

ユーザ機器認証サーバ３００とショップサーバ１００間の相互認証～暗号化コンテンツ鍵データ（ＤＡＳ）送信～ショップサーバにおける受信データ検証。

Ｄ．ショップサーバとユーザ機器間における処理（図１に示す（１４）～（１９）の処理）

ユーザ機器２００とショップサーバ１００の相互認証～ユーザ機器２００からショップサーバ１００に対する暗号化コンテンツ鍵要求データ送信～ショップサーバ１００からユーザ機器２００に対する鍵２（ショップ）の送信～ユーザ機器２００における受信データ検証。

【０１３２】まず、Ａ．ショップサーバとユーザ機器間における処理（図１に示す（１）～（６）の処理）について、図２３、図２４を用いて説明する。

【０１３３】図２３、図２４において、左側がショップサーバの処理、右側がユーザ機器の処理を示す。なお、すべてのフローにおいて、ショップサーバの処理ステップＮｏをＳ１０ｘｘ、ユーザ機器の処理ステップＮｏをＳ２０ｘｘ、ユーザ機器認証サーバの処理ステップＮｏをＳ３０ｘｘとして示す。

【０１３４】まず、図２３に示すように、処理開始時に、ショップサーバとユーザ機器間において相互認証が実行される（Ｓ１００１，Ｓ２００１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ショップサーバは、購買管理データベース（図３参照）に新規ショップ処理ＮＯを新たな処理エントリとして追加（Ｓ１００３）する。

【０１３５】一方、ユーザ機器は、相互認証が成立すると、今回のコンテンツ取り引きにおいて適用するトランザクションＩＤを例えば乱数に基づいて生成し、購入データベース（図８参照）に新規トランザクションＩＤを新たなエントリとして追加（Ｓ２００３）する。さらに、ユーザ機器は、ショップサーバに対するコンテンツ購入要求データの送信（Ｓ２００４）、すなわち、図１４（ａ）に示す（３）購入要求データの送信を実行する。

【０１３６】ショップサーバは、ユーザ機器からのコンテンツ購入要求データを受信（Ｓ１００４）し、受信データ（Ｓ１００５）の検証を実行する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信ＯＫのレスポンスを送信（Ｓ１００８）し、購買管理データベースのステータスを「購入受付完了」に設定（Ｓ１０１０）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信ＮＧのレスポンスを送信（Ｓ１００７）し、購買管理データベースのステータスを「購入受付失敗」に設定（Ｓ１００９）する。

【０１３７】ユーザ機器は、ショップサーバからの受信ＯＫのレスポンスを受信（Ｓ２００５，Ｓ２００６でＹｅｓ）すると、購入管理データベースのステータスを「購入要求送信完了」に設定し、ショップサーバからの受信ＮＧレスポンスを受信（Ｓ２００５，Ｓ２００６でＮｏ）すると、購入管理データベースのステータスを「購入要求送信失敗」に設定する。

【０１３８】ショップサーバでは、購買管理データベースのステータスを「購入受付完了」に設定（Ｓ１０１０）後、暗号化コンテンツ鍵データ１（ショップ）（図１４（ｂ）参照）を生成（Ｓ１０１１）し、ユーザ機器に対して、コンテンツ鍵：Ｋｃで暗号化した暗号化コンテンツ：Ｋｃ（Content）を送信（Ｓ１０１２）し、さらに、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を送信（Ｓ１０１３）する。

【０１３９】ユーザ機器は、購入管理データベースのステータスを「購入要求送信完了」に設定（Ｓ２００７）後、ショップサーバから、コンテンツ鍵：Ｋｃで暗号化した暗号化コンテンツ：Ｋｃ（Content）を受信（Ｓ２００９）し、さらに、ショップサーバから暗号化コンテンツ鍵データ１（ショップ）（図１４（ｂ））を受信（Ｓ２０１０）する。

【０１４０】ユーザ機器は、ステップＳ２００９，Ｓ２０１０で受信したデータの検証処理（図１１参照）を実行（Ｓ２０２１）し、受信データの検証により、データが改竄のない正当なデータであると認められると、ショップサーバに対して受信ＯＫのレスポンスを送信（Ｓ２０２３）し、購入管理データベースのステータスを「鍵１受信完了」に設定（Ｓ２０２５）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ショップサーバに対して受信ＮＧのレスポンスを送信（Ｓ２０２４）し、購入管理データベースのステータスを「鍵１受信失敗」に設定（Ｓ２０２６）した後、ショップサーバとの接続を切る（Ｓ２０２７）。

【０１４１】ショップサーバは、ユーザ機器からのレスポンスを受信（Ｓ１０２１）し、レスポンスがＯＫである場合は、購買管理データベースのステータスを「鍵１配信成功」に設定（Ｓ１０２４）する。レスポンスがＮＧである場合は、購買管理データベースのステータスを「鍵１配信失敗」に設定（Ｓ１０２３）した後、ユーザ機器との接続を切る（Ｓ１０２５）。

【０１４２】なお、ステップＳ１００２，Ｓ２００２の相互認証失敗の場合、Ｓ１００９のステータスの「購入受付失敗」の設定、および、Ｓ２００８のステータスの「購入要求送信失敗」の設定の場合は、いずれも処理を中止して、接続を切る処理を行なって処理終了とする。

【０１４３】次に、Ｂ．ユーザ機器認証サーバとユーザ機器間における処理（図１に示す（７）～（９）の処理）について、図２５のフローに従って説明する。

【０１４４】まず、ユーザ機器認証サーバとユーザ機器間において相互認証が実行される（Ｓ３００１，Ｓ２０３１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器認証サーバは、ライセンス管理データベース（図６参照）に新規ユーザ機器認証サーバ処理ＮＯ、を新たな処理エントリとして追加（Ｓ３００３）する。

【０１４５】一方、ユーザ機器は、相互認証が成立すると、暗号化コンテンツ鍵データ（ユーザ機器）（図１４（ｃ）参照）を生成（Ｓ２０３３）し、ユーザ機器認証サーバへ送信（Ｓ２０３４）する。

【０１４６】ユーザ機器認証サーバは、ユーザ機器からの暗号化コンテンツ鍵データ（ユーザ機器）を受信（Ｓ３００４）し、受信データの検証（Ｓ３００５）を実行する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信ＯＫのレスポンスを送信（Ｓ３００８）し、ライセンス管理データベースのステータスを「鍵受信完了」に設定（Ｓ３０１０）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信ＮＧのレスポンスを送信（Ｓ３００７）し、ライセンス管理データベースのステータスを「鍵受信失敗」に設定（Ｓ３００９）後、ユーザ機器との接続を切る（Ｓ３０１１）。

【０１４７】ユーザ機器は、ユーザ機器認証サーバからの受信ＯＫのレスポンスを受信（Ｓ２０３５，Ｓ２０３６でＹｅｓ）すると、購入管理データベースのステータスを「鍵送信完了」に設定（Ｓ２０３７）し、ユーザ機器認証サーバからの受信ＮＧレスポンスを受信（Ｓ２０３５，Ｓ２０３６でＮｏ）すると、購入管理データベースのステータスを「鍵送信失敗」に設定（Ｓ２０３８）した後、ユーザ機器認証サーバとの接続を切る（Ｓ２０３９）。

【０１４８】なお、ステップＳ３００２，Ｓ２０３２の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【０１４９】次に、Ｃ．ユーザ機器認証サーバとショップサーバ間における処理（図１に示す（１１）～（１３）の処理）について、図２６のフローに従って説明する。

【０１５０】まず、ユーザ機器認証サーバとショップサーバ間において相互認証が実行される（Ｓ３０２１，Ｓ１０３１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器認証サーバは、暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）参照）を生成（Ｓ３０２３）し、ショップサーバに送信（Ｓ３０２４）する。

【０１５１】一方、ショップサーバは、相互認証の成立後、ユーザ機器認証サーバから暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）参照）を受信（Ｓ１０３

３）し、受信データの検証（Ｓ１０３４）を実行する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器認証サーバに対して受信ＯＫのレスポンスを送信（Ｓ１０３６）し、購買管理データベースのステータスを「鍵受信完了」に設定（Ｓ１０３８）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器認証サーバに対して受信ＮＧのレスポンスを送信（Ｓ１０３７）し、購買管理データベースのステータスを「鍵受信失敗」に設定（Ｓ１０３９）後、ユーザ機器認証サーバとの接続を切る（Ｓ１０４０）。

【０１５２】ユーザ機器認証サーバは、ショップサーバからの受信ＯＫのレスポンスを受信（Ｓ３０２５，Ｓ３０２６でＹｅｓ）すると、ライセンス管理データベースのステータスを「鍵送信完了」に設定（Ｓ３０２８）し、ショップサーバからの受信ＮＧレスポンスを受信（Ｓ３０２５，Ｓ３０２６でＮｏ）すると、ライセンス管理データベースのステータスを「鍵送信失敗」に設定（Ｓ３０２７）した後、ユーザ機器認証サーバとの接続を切る（Ｓ３０２９）。

【０１５３】なお、ステップＳ３０２２，Ｓ１０３２の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【０１５４】次に、Ｄ．ショップサーバとユーザ機器間における処理（図１に示す（１４）～（１９）の処理）について、図２７、図２８を用いて説明する。

【０１５５】まず、処理開始時に、ショップサーバとユーザ機器間において相互認証が実行される（Ｓ１０５１，Ｓ２０５１）。相互認証処理は、図１２または図１３を用いて説明した処理として実行される。相互認証処理において生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。相互認証が成立すると、ユーザ機器は、暗号化コンテンツ鍵送信要求データ（図１７（ｅ）参照）を生成（Ｓ２０５３）し、ショップサーバへ送信（Ｓ２０５４）する。

【０１５６】ショップサーバは、ユーザ機器からの暗号化コンテンツ鍵送信要求データを受信（Ｓ１０５４）し、受信データの検証を実行（Ｓ１０５５）する。データ検証は、先に説明した図１１の処理フローに従った処理である。受信データの検証により、データが改竄のない正当なデータであると認められると、ユーザ機器に対して受信ＯＫのレスポンスを送信（Ｓ１０５８）し、購買管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定（Ｓ１０６０）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ユーザ機器に対して受信ＮＧのレスポンスを送信（Ｓ１０５７）し、購買管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付失敗」に設定（Ｓ１０５９）する。

【０１５７】ユーザ機器は、ショップサーバからの受信ＯＫのレスポンスを受信（Ｓ２０５５，Ｓ２０５６でＹｅｓ）すると、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定（Ｓ２０５７）し、ショップサーバからの受信ＮＧレスポンスを受信（Ｓ２０５５，Ｓ２０５６でＮｏ）すると、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信失敗」に設定（Ｓ２０５８）する。

【０１５８】ショップサーバでは、購買管理データベースのステータスを「暗号化コンテンツ鍵送信要求受付完了」に設定（Ｓ１０６０）後、暗号化コンテンツ鍵データ２（ショップ）（図１７（ｆ）参照）を生成（Ｓ１０６１）し、ユーザ機器に対して、図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）を送信（Ｓ１０６２）する。

【０１５９】ユーザ機器は、購入管理データベースのステータスを「暗号化コンテンツ鍵送信要求送信完了」に設定（Ｓ２０５７）後、ショップサーバから、暗号化コンテンツ鍵データ２（ショップ）（図１７（ｆ））を受信（Ｓ２０５９）する。

【０１６０】ユーザ機器は、ステップＳ２０５９で受信したデータの検証処理（図１１参照）を実行（Ｓ２０７１）し、受信データの検証により、データが改竄のない正当なデータであると認められると、ショップサーバに対して受信ＯＫのレスポンスを送信（Ｓ２０７３）し、購入管理データベースのステータスを「鍵２受信完了」に設定（Ｓ２０７５）する。受信データの検証により、データが改竄のある不当なデータであると認められると、ショップサーバに対して受信ＮＧのレスポンスを送信（Ｓ２０７４）し、購入管理データベースのステータスを「鍵２受信失敗」に設定（Ｓ２０７６）した後、ショップサーバとの接続を切る（Ｓ２０７７）。

【０１６１】ショップサーバは、ユーザ機器からのレスポンスを受信（Ｓ１０７１）し、レスポンスがＯＫである場合は、購買管理データベースのステータスを「鍵２配信成功」に設定（Ｓ１０７４）する。レスポンスがＮＧである場合は、購買管理データベースのステータスを「鍵２配信失敗」に設定（Ｓ１０７３）した後、ユーザ機器との接続を切る（Ｓ１０７５）。

【０１６２】なお、ステップＳ１０５２，Ｓ２０５２の相互認証失敗の場合は、処理を中止して、接続を切る処理を行なって処理終了とする。

【０１６３】［基本コンテンツ配信モデル１の変形例］ここまで、図１に示した基本コンテンツ配信モデル１の構成に基づいてコンテンツ購入処理の構成、処理手順について説明してきたが、基本的にユーザ機器認証サーバにおいてコンテンツ鍵のかけかえ処理を実行する構成とするポリシーを持つ構成であれば、図１に示す構成に限らず、様々な態様が実現可能である。以下、様々な変形

例について説明する。

【０１６４】図２９に示す構成は、ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成である。ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領するが、ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。本例では、各エンティテイ間で相互認証処理を省略しているが、基本コンテンツ配信モデル１同様、相互認証処理を行なっても構わない。

【０１６５】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図２９の処理（３））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図２９の処理（４））する。配信サーバ４００は、ショップサーバ１００からのコンテンツ配信要求データを検証し、データの正当性が確認された場合、コンテンツデータベース４１０から取り出した暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を送信（図２９の処理（６））する。暗号化コンテンツ鍵データ（配信サーバ）は、前述の実施例の暗号化コンテンツ鍵データ１（ショップ）に対応し、ユーザ機器認証サーバの公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵Ｋｃ、すなわちＫｐＤＡＳ（Ｋｃ）を含むデータである。

【０１６６】ユーザ機器２００が配信サーバ４００から暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を受信した以後の処理は、先の図１に示した構成に基づく実施例と同様となる。

【０１６７】本構成においては、ショップサーバ１００は、ユーザ機器からのコンテンツ要求を受け付けて、その正当性を検証する機能、ユーザ機器認証サーバからの、かけかえ済みの暗号化コンテンツ鍵を受信し、ユーザ機器に対する配信を主として実行し、コンテンツ自体の管理、配信を行なわない。従って、例えば音楽データを管理する音楽コンテンツ配信サーバ、ゲームコンテンツを管理するゲームコンテンツ配信サーバ等、様々なコンテンツ管理主体となる複数の配信サーバに対して１つのショップサーバがユーザ機器からのコンテンツ要求に応答し、ショップサーバが要求に応じて要求コンテンツを管理する配信サーバにコンテンツ配信要求を送信する構成に適した態様である。また、この構成にしたことにより、例えば、ユーザ機器とショップサーバは双方向通信であるため、インターネットを使うが、配信サーバからユーザ機器へは片方向通信であるため、高速な衛星通信が利用できるメリットがある。

【０１６８】図３０は、図２９と同様ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成であり、ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領するが、ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。図２９の構成と異なる点は、ショップサーバ１００から配信サーバ４００に対してコンテンツ配信要求を送信せず、ユーザ機器認証サーバ３００が、配信サーバ４００に対してコンテンツ配信要求を送信する構成とした点である。

【０１６９】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図３０の処理（３））を行なって、要求データの正当性を確認した後、ユーザ機器認証サーバ３００に対して、コンテンツ配信要求の送信を実行（図３０の処理（４））する。その後、ユーザ機器認証サーバ３００は、データの検証（図３０の処理（５））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図３０の処理（６））する。配信サーバ４００は、ユーザ機器認証サーバ３００からのコンテンツ配信要求データを検証し、正当性が確認された場合、ユーザ機器２００に対して、コンテンツデータベース４１０から取り出した暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を送信（図３０の処理（８））する。暗号化コンテンツ鍵データ（配信サーバ）は、前述の実施例の暗号化コンテンツ鍵データ１（ショップ）に対応し、ユーザ機器認証サーバの公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵Ｋｃ、すなわちＫｐＤＡＳ（Ｋｃ）を含むデータである。

【０１７０】ユーザ機器２００が配信サーバ４００から暗号化コンテンツおよび暗号化コンテンツ鍵データ（配信サーバ）を受信した以後の処理は、先の図１に示した構成に基づく実施例と同様となる。

【０１７１】本構成においては、ユーザ機器認証サーバ３００は、ユーザ機器２００からの鍵のかけかえ要求以前、ショップサーバ１００に対してコンテンツ購入要求があった時点で、コンテンツ購入要求主体であるユーザ機器情報を取得し、管理することが可能となる。従って、ユーザ機器２００からの鍵のかけかえ要求受領時に、すでに登録済みのコンテンツ購入要求ユーザ機器であるか否かの照合処理が可能となる。

【０１７２】［１．３．基本コンテンツ配信モデル２］

次に、図３１を用いて基本コンテンツ配信モデル１と異なる基本コンテンツ配信モデル２について説明する。基本コンテンツ配信モデル２では、ユーザ機器２００とユーザ機器認証サーバ３００との間ではデータ送受信が行われない。図３１に示す各処理（１）～（１９）について、基本コンテンツ配信モデル１との相違点を中心に説明する。なお、本実施例では、エンティテイ間の通信において相互認証処理（（１）、（７）、（１３））を行なったものを述べているが、必要に応じて省略しても構わない。

【０１７３】（１）相互認証

コンテンツをショップサーバ１００から購入しようとするユーザ機器２００は、ショップサーバ１００との間で

相互認証処理を行なう。相互認証処理は、図１２または図１３を用いて説明した処理である。相互認証処理において、生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。

【０１７４】（２）トランザクションＩＤ、購入要求データ生成、および

（３）購入要求データ送信

ショップサーバ１００とユーザ機器２００間の相互認証が成功すると、ユーザ機器２００は、コンテンツの購入要求データを生成する。購入要求データの構成を図３２（ｇ）に示す。購入要求データは、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、コンテンツ取り引きの識別子として、ユーザ機器２００の暗号処理手段が乱数に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ショップ側に送付済みの場合は、必ずしも改めて送付する必要はない。

【０１７５】（４）受信データ検証

図３２（ｇ）に示す購入要求データをユーザ機器２００から受信したショップサーバ１００は、受信データの検証処理を実行する。検証処理の詳細は、先に図１５を用いて説明した通りである。

【０１７６】（５）暗号化コンテンツおよび購入受付データ送信

ショップサーバ１００において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定すると、ショップサーバ１００は、暗号化コンテンツおよび購入受付データをユーザ機器に送信する。これらは、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Ｋｃ（content）と、購入要求を受け付けたことを示すのみのデータであり、先のコンテンツキー：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵で暗号化した暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を含まないデータである。

【０１７７】購入受付データの構成を図３２（ｈ）に示す。購入受付データは、コンテンツ購入の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、購入要求データ（図３２（ｇ）のユーザ機器公開鍵証明書を除いたデータ）、コンテンツ取り引きに伴いショップサーバ１００が生成したショップ処理Ｎｏ．を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、購入受付データには、ショップサーバ１００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【０１７８】（６）受信データ検証

ショップサーバ１００から暗号化コンテンツ：Ｋｃ（content）と、図３２（ｈ）に示す購入受付データを受信したユーザ機器２００は、購入受付データの検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図３２（ｈ）に示す購入受付データのショップ署名の検証を実行する。

【０１７９】（７）相互認証

（８）暗号化コンテンツ鍵データ１（ショップ）送信

次にショップサーバ１００は、ユーザ機器認証サーバ３００にアクセスし、ショップサーバ１００と、ユーザ機器認証サーバ３００間において相互認証処理を実行する。相互認証が成立すると、ショップサーバ１００は、ユーザ機器認証サーバ３００に対して、暗号化コンテンツ鍵データ１（ショップ）を送信する。

【０１８０】暗号化コンテンツ鍵データ１（ショップ）の構成を図３２（ｉ）に示す。暗号化コンテンツ鍵データ１（ショップ）は、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ３００の識別子であるユーザ機器認証サーバＩＤ、ユーザ機器２００から受領した購入要求データ（図３２（ｇ）のユーザ機器公開鍵証明書を除いたデータ）、ショップ処理Ｎｏ．を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ１（ショップ）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器２００の公開鍵証明書が添付され、ユーザ機器認証サーバ３００に送付される。なお、ユーザ機器認証サーバ３００がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０１８１】（９）受信データ検証

ショップサーバ１００から暗号化コンテンツ鍵データ１（ショップ）（図３２（ｉ））を受信したユーザ機器認証サーバ３００は、受信データの検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器認証サーバ３００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図３２（ｉ）に示す暗号化コンテンツ鍵データ１（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実

行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図３２（ｉ）に示す暗号化コンテンツ鍵データ１（ショップ）に含まれる（３）購入要求データのユーザ機器署名の検証を実行する。

【０１８２】（１０）暗号化コンテンツ鍵かけかえ処理

ユーザ機器認証サーバ３００において、ショップサーバ１００から受信した暗号化コンテンツ鍵データ１（ショップ）の検証が終了し、正当なデータであると判定すると、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ１（ショップ）に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）３００の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ３００の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。この処理は、先に説明した図１６に示すフローに従った処理である。

【０１８３】（１１）暗号化コンテンツデータ送信

次に、ユーザ機器認証サーバ３００は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００に送信する。

【０１８４】暗号化コンテンツ鍵データ（ＤＡＳ）の構成を図３３（ｊ）に示す。暗号化コンテンツ鍵データ（ＤＡＳ）は、コンテンツ購入の要求先であるショップサーバ１００の識別子であるショップＩＤ、暗号化コンテンツ鍵データ１（ショップ）（図３２（ｉ）のショップおよびユーザ機器公開鍵証明書を除いたデータ）、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ３００が生成した暗号化コンテンツ鍵データ：ＫｐＤＥＶ（Ｋｃ）を有し、これらのデータに対するユーザ機器認証サーバ３００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ＤＡＳ）には、ユーザ機器認証サーバ３００と、ユーザ機器２００の公開鍵証明書が添付され、ショップサーバ１００に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【０１８５】また、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ（ＤＡＳ）は、図３３（ｊ）に示すような（８）暗号化コンテンツ鍵データ１（ショップ）をそのまま含むデータ構成とすることなく、図３４（ｊ’）に示すように、ショップＩＤ、ユーザ機器ＩＤ、トランザクションＩＤ、コンテンツＩＤ、ショップ処理ＮＯ、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）の各データを、ユーザ機器認証サーバ３００が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ（ＤＡＳ）としてもよい。添付する公開鍵証明書は、ユーザ機器認証サーバ３００の公開鍵証明書である。

【０１８６】（１２）受信データ検証

ユーザ機器認証サーバ３００から暗号化コンテンツ鍵データ（ＤＡＳ）（図３３（ｊ））を受信したショップサーバ１００は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ショップサーバ１００は、まずユーザ機器認証サーバ３００から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図３３（ｊ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行する。なお、先に説明した図３４（ｊ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１００が受領した場合も同様の検証を実行する。さらに、必要に応じて図３３（ｊ）の暗号化コンテンツデータ（ＤＡＳ）内の暗号化コンテンツ鍵１（ショップ１）を検証するようにしてもよい。

【０１８７】（１３）相互認証、および

（１４）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器２００は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証を実行して、相互認証が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器２００からショップサーバ１００に送信される。

【０１８８】（１５）検証処理、および

（１６）課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１００は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図１５を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ１００は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【０１８９】前述した基本モデル１と同様、この課金処理に至るまでには、ユーザ機器認証サーバ３００による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ１００は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器２００においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵か

けかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【０１９０】（１７）暗号化コンテンツ鍵データ２（ショップ）送信

ショップサーバ１００における課金処理が終了すると、ショップサーバ１００は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器２００に送信する。

【０１９１】暗号化コンテンツ鍵データ２（ショップ）の構成を図３３（ｋ）に示す。暗号化コンテンツ鍵データ２（ショップ）は、暗号化コンテンツ鍵要求の要求元であるユーザ機器２００の識別子であるユーザ機器ＩＤ、ユーザ機器認証サーバ３００から受領した暗号化コンテンツ鍵データ（ＤＡＳ）（図３３（ｊ）のユーザ機器認証サーバ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するショップサーバ１００の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ２（ショップ）には、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書が添付され、ユーザ機器２００に送付される。なお、ユーザ機器２００がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０１９２】なお、ユーザ機器認証サーバ３００が信頼できる第三者機関であると認められる存在であり、ショップサーバ１００がユーザ機器認証サーバ３００から受信する暗号化コンテンツ鍵データ（ＤＡＳ）が先に説明した図３４（ｊ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）である場合は、ショップサーバ１００は、図３４（ｋ’）に示す暗号化コンテンツ鍵データ２（ショップ）をユーザ機器に送付する。すなわち、図３４（ｊ’）に示す簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）にショップサーバの署名を付加したデータに、ショップサーバ１００の公開鍵証明書と、ユーザ機器認証サーバ３００の公開鍵証明書を添付してユーザ機器２００に送付する。

【０１９３】（１８）受信データ検証

ショップサーバ１００から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器２００は、まずショップサーバ１００から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバ１００の公開鍵ＫｐＳＨＯＰを用いて図３３（ｋ）に示す暗号化コンテンツ鍵データ２（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ３００の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ３００の公開鍵ＫｐＤＡＳを用いて図３３（ｊ）に示す暗号化コンテンツ鍵データ２（ショップ）に含まれる（１１）暗号化コンテンツ鍵データ（ＤＡＳ）の署名検証を実行する。さらに、必要に応じて図３３（ｊ）の暗号化コンテンツデータ（ＤＡＳ）内の暗号化コンテンツ鍵１（ショップ１）を検証するようにしてもよい。

【０１９４】（１９）保存処理

ショップサーバ１００から受信した暗号化コンテンツ鍵データ２（ショップ）を検証したユーザ機器２００は、暗号化コンテンツ鍵データ２（ショップ）に含まれる自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器２００の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０１９５】このように、基本配信モデル２においては、ユーザ機器２００と、ユーザ機器認証サーバ３００との間ではデータの送受信が実行されず、ユーザ機器２００は、ショップサーバ１００との間でデータ送受信を行なうのみでよく、ユーザ機器の処理負担が軽減される。

【０１９６】［１．２．基本コンテンツ配信モデル２の変形例］次に、図３１に示した基本コンテンツ配信モデル２の構成の変形例について説明する。図３５に示す構成は、ショップサーバの機能を分離し、ショップサーバと配信サーバを設けた構成である。ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領するが、ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。本構成では、データ送受信を実行するエンティテイ間での相互認証を行なわず、各エンティテイは、受信データの署名検証のみを行なう。しかし、基本コンテンツ配信モデル２同様、エンティテイ間で相互認証処理を行なう構成をとっても構わない。

【０１９７】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図３５の処理（３））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図３５の処理（４））する。配信サーバ４００は、ショップサーバ１００からのコンテンツ配信要求データを検証し、データの正当性が確認された

場合、コンテンツデータベース４１０から取り出した暗号化コンテンツを送信（図３５の処理（６））する。

【０１９８】ユーザ機器２００は、配信サーバ４００から、暗号化コンテンツを受信し、データ検証の後、暗号化コンテンツ受領データを配信サーバ４００に送信（図３５の処理（８））する。配信サーバ４００は、受信データ検証の後、ユーザ機器認証サーバ３００に対して暗号化コンテンツ鍵データ（配信サーバ）および暗号化コンテンツ鍵かけかえ要求を送信（図３５の処理（１０））する。

【０１９９】ユーザ機器認証サーバ３００が配信サーバ４００から暗号化コンテンツ鍵データ（配信サーバ）および暗号化コンテンツ鍵かけかえ要求を受信した以後の処理は、相互認証処理を省略した以外は、先の図３１に示した構成に基づく実施例と同様となる。

【０２００】本構成においては、ユーザ機器は、相互認証を行なわずに、ショップサーバに対してコンテンツ購入要求を送信し、配信サーバから暗号化コンテンツを受領する。ショップサーバ１００は、ユーザ機器からのコンテンツ要求を受け付けて、その正当性を署名検証のみに基づいて検証する。さらに、ユーザ機器認証サーバからの、かけかえ済みの暗号化コンテンツ鍵を受信し、その正当性を署名検証により実行する。配信サーバ４００は、ショップサーバからの受信データについての署名検証を実行してデータ正当性の確認を行ないコンテンツ配信を行なう。

【０２０１】ショップサーバ１００は、コンテンツ自体の管理、配信を行なわない。従って、例えば音楽データを管理する音楽コンテンツ配信サーバ、ゲームコンテンツを管理するゲームコンテンツ配信サーバ等、様々なコンテンツ管理主体となる複数の配信サーバに対して１つのショップサーバがユーザ機器からのコンテンツ要求に応答し、ショップサーバが要求に応じて要求コンテンツを管理する配信サーバにコンテンツ配信要求を送信する構成に適した態様である。また、この構成にしたことにより、例えば、ユーザ機器とショップサーバは双方向通信であるため、インターネットを使うが、配信サーバからユーザ機器へは片方向通信であるため、高速な衛星通信が利用できるメリットがある。

【０２０２】本実施例では、相互認証が省略され、署名検証のみにより、データの正当性を確認する処理としたので、処理の効率化が実現される。

【０２０３】図３６は、図３５と同様ショップサーバの機能を分離し、ショップサーバと配信サーバを設け、相互認証を省略した構成であり、ショップサーバ１００は、ユーザ機器２００からのコンテンツ購入要求を受領し、署名検証を行なう。ユーザ機器２００に対するコンテンツ配信は配信サーバ４００が実行する。図３５の構成と異なる点は、ショップサーバ１００から配信サーバ４００に対してコンテンツ配信要求を送信せず、ユーザ機器認証サーバ３００が、配信サーバ４００に対してコンテンツ配信要求を送信する構成とした点である。

【０２０４】ショップサーバ１００は、ユーザ機器２００からの購入要求データを受信し、データの検証（図３６の処理（３））を行なって、要求データの正当性を確認した後、ユーザ機器認証サーバ３００に対して、暗号化コンテンツ鍵データ１（ショップ）の送信を実行（図３６の処理（４））する。その後、ユーザ機器認証サーバ３００は、データの検証（図３６の処理（５））を行なって、要求データの正当性を確認した後、配信サーバ４００に対して、コンテンツ配信要求の送信を実行（図３６の処理（６））する。配信サーバ４００は、ユーザ機器認証サーバ３００からのコンテンツ配信要求データを検証し、正当性が確認された場合、ユーザ機器２００に対して、コンテンツデータベース４１０から取り出した暗号化コンテンツを送信（図３６の処理（８））する。以後の処理は、先の図３５に示した構成に基づく処理と同様となる。

【０２０５】本構成においては、ユーザ機器認証サーバ３００は、配信サーバ４００からの鍵のかけかえ要求以前、ショップサーバ１００に対してコンテンツ購入要求があった時点で、コンテンツ購入要求主体であるユーザ機器情報を取得し、管理することが可能となる。従って、配信サーバ４００からの鍵のかけかえ要求受領時に、すでに登録済みのコンテンツ購入要求ユーザ機器であるか否かの照合処理が可能となる。また、ＤＡＳが信頼できる機関であるとみなせば、配信サーバはショップサーバの送信データを検証しなくてもよくなり、処理の効率化が図れる。

【０２０６】以上、説明したように、本発明のコンテンツ配信構成によれば、ユーザ機器は、暗号化コンテンツＫｃ（Content）取得後、コンテンツ利用可能な状態に至るまでには、ユーザ機器認証サーバにおける暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となる。従って、ショップサーバが、ユーザ機器に対して、ユーザ機器認証サーバに通知せずコンテンツを販売し、コンテンツをユーザ機器において利用可能な状態とすることができない。ユーザ機器認証サーバは、ユーザ機器認証サーバ・ライセンス管理データベース（図６参照）に、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべてのショップの取り引きの管理が可能であり、課金されたコンテンツ取り引きを把握し、ショップの課金処理において受領されたコンテンツ料金を、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に正確に配分することが可能となり、不正なコンテンツ利用を排除する構成が実現される。

【０２０７】［２．電子チケットを利用したコンテンツ配信モデル］次に、ユーザによるコンテンツの利用（購入）に基づいて、コンテンツの著作権者、製作者、ライ

センスホルダー、ショップ等、様々な関係者に対する利益配分情報を記述した電子チケットを発行して、発行した電子チケットに基づく利益配分処理を実行する構成について説明する。

【０２０８】図３７に電子チケットに基づく利益配分を実行するシステム構成を示す。図３７のコンテンツ配信システムは、ユーザ機器が購入するコンテンツの購入要求を受け付け、コンテンツ購入に伴う利用料金の利益配分情報を記述した電子チケットを発行するチケット発行サーバ（ＴＩＳ：Ticket Issuer Server）６１０、コンテンツ購入主体となるユーザ機器（ＤＥＶ）６２０、正当なコンテンツ取り引き管理のための鍵かけかえ処理を行なう管理サーバとして機能するユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）６３０、コンテンツの配信を行なうコンテンツプロバイダ（ＣＰ）等の配信サーバ（ＣＰ：Content Provider）６４０、さらに、電子チケットに基づいて利用料金の振替等の換金処理を行なうチケット換金サーバ（ＴＥＳ：Ticket Exchange Server）６５０を主構成要素とする。

【０２０９】（チケット発行サーバ）図３７のコンテンツ配信システムのチケット発行サーバ（ＴＩＳ）６１０の構成を図３８に示す。チケット発行サーバ６１０は、ユーザ機器６２０からの購入要求を受け付け、購入要求のあった取り引き対象となるコンテンツに対応してその利益配分情報を記述した電子チケットを発行する。

【０２１０】チケット発行サーバ（ＴＩＳ）６１０は、コンテンツ取り引きに伴う発行チケットの管理データ、例えばコンテンツ販売先のユーザ機器の識別子とコンテンツ識別子、コンテンツ料金等を対応づけて管理するチケット発行管理データベース６１２を有する。さらに、ユーザ機器６２０からのコンテンツ購入要求検証、チケット発行管理データベースの制御、チケットに基づくユーザ機器に対する課金処理、ユーザ機器等との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６１３を有する。

【０２１１】チケット発行管理データベース６１２のデータ構成を図３９に示す。チケット発行管理データベース６１２は、チケット発行サーバがコンテンツ取り引きに応じてチケット発行処理を実行する際に内部生成する識別番号としてのチケット発行処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、ユーザ機器とチケット発行サーバ間での取り引きを実行する際に、コンテンツ取り引き識別子としてユーザ機器で生成発行するトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、チケット発行サーバ６１０の発行する電子チケットに基づいて対価を得るエンティテイ、例えば著作権者、ライセンスホルダ、管理者、コンテンツ販売関係者等の識別子としてのチケット利用先ＩＤ、各チケット利用先ＩＤに対応するコンテンツ利用料金配分金額としての金額、チケットに基づく換金処理の有効期限、チケット発行サーバ６１０におけるチケット発行、管理処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２１２】チケット発行サーバ６１０の制御手段６１３は、図３８に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段６１３は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段６１３の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。チケット発行サーバ６１０が格納する暗号鍵等の暗号処理用データとしては、チケット発行サーバ６１０の秘密鍵：ＫｓＴＩＳ、チケット発行サーバ６１０の公開鍵証明書Ｃｅｒｔ＿ＴＩＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２１３】制御手段６１３の構成は、先に図４を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置（ＣＰＵ:Central Processing Unit）、ＲＯＭ（Read only Memory）、ＲＡＭ（Random Access Memory）、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【０２１４】（ユーザ機器）ユーザ機器（ＤＥＶ）６２０は、図１の構成におけるユーザ機器、すなわち、図７の構成と同様の構成を持つ。ユーザ機器６２０が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器の秘密鍵：ＫｓＤＥＶ、ユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡ、コンテンツをユーザ機器の例えばハードディスク等の記憶手段に格納する際の暗号化鍵として適用する保存鍵Ｋｓｔｏがある。

【０２１５】図３７のチケット管理構成を実行するシステムにおけるユーザ機器６２０の有する購入管理データベースは、チケット管理機能を持つデータ構成となる。購入管理データベースのデータ構成を図４０に示す。購入管理データベースは、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、チケットを送信した先の送信先エンティテイの識別子としてのチケット送信先ＩＤ、さらに、ユーザ機器におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２１６】（ユーザ機器認証サーバ）ユーザ機器認証サーバ（ＤＡＳ）６３０は、図１の構成におけるユーザ機器認証サーバ、すなわち、図５の構成と同様の構成を持つ。ユーザ機器認証サーバ６３０が格納する暗号鍵等の暗号処理用データとしては、ユーザ機器認証サーバ（ＤＡＳ）の秘密鍵：ＫｓＤＡＳ、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵証明書Ｃｅｒｔ＿ＤＡＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２１７】図３７のチケット管理構成を実行するシステムにおけるユーザ機器認証サーバ６３０の有するライセンス管理データベースは、チケット管理機能を持つデータ構成となる。ライセンス管理データベースのデータ構成を図４１に示す。ライセンス管理データベースは、コンテンツ取り引き時にユーザ機器認証サーバ（ＤＡＳ）６３０の実行する処理に応じて内部生成する処理識別子としてのユーザ機器認証サーバ処理Ｎｏ．、コンテンツ購入依頼を発行したユーザ機器の識別子である機器ＩＤ、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションＩＤ、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、さらに、ユーザ機器認証サーバ（ＤＡＳ）におけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２１８】（配信サーバ）図３７のコンテンツ配信システムの配信サーバ６４０の構成を図４２に示す。配信サーバ６４０は、例えばコンテンツプロバイダ（ＣＰ）であり、取り引き対象となるコンテンツをコンテンツキーで暗号化した暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）と、コンテンツキーＫｃをユーザ機器認証サーバ（ＤＡＳ：Device Authentication Server）の公開鍵：ＫｐＤＡＳで暗号化した暗号化コンテンツキーＫｐＤＡＳ（Ｋｃ）を格納したコンテンツデータベース６４４を有する。なお、暗号化コンテンツデータであるＫｃ（Ｃｏｎｔｅｎｔ）は、図にも示すように、それぞれコンテンツ識別子であるコンテンツＩＤが付加され、コンテンツＩＤに基づいて識別可能な構成を持つ。

【０２１９】配信サーバ６４０は、さらにコンテンツの配信管理データを管理する配信管理データベース６４２を有する。配信管理データベース６４２は、チケット管理機能を持つデータ構成となる。購入管理データベースのデータ構成を図４３に示す。配信管理データベース６４２は、コンテンツ配信処理を実行する際に、配信サーバ６４０が設定する配信サーバ処理Ｎｏ．、取り引き対象コンテンツの識別子であるコンテンツＩＤ、コンテンツの配信対象識別子としてのユーザ機器ＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行体が設定するチケット発行処理Ｎｏ．、さらに、配信サーバにおけるコンテンツ取り引き処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される

【０２２０】さらに、配信サーバ６４０は、コンテンツデータベース６４４からの配信コンテンツの抽出処理、取り引きに伴う配信管理データベース６４２に対して登録する取り引きデータの生成処理、ユーザ機器６２０他との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６４３を有する。制御手段６４３は、図４２に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段６４３は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段６４３の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。配信サーバ６４０が格納する暗号鍵等の暗号処理用データとしては、配信サーバ６４０の秘密鍵：ＫｓＣＰ、配信サーバ６４０の公開鍵証明書Ｃｅｒｔ＿ＣＰ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２２１】制御手段６４３の構成は、先に図４を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置（ＣＰＵ:Central Processing Unit）、ＲＯＭ（Read only Memory）、ＲＡＭ（Random Access Memory）、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【０２２２】（チケット換金サーバ）図３７のコンテンツ配信システムのチケット換金サーバ（ＴＥＳ）６５０の構成を図４４に示す。チケット換金サーバ６５０は、様々なエンティテイから電子チケットを受信し、受信データの検証の後、チケットに基づく換金処理、例えば口座振替処理、あるいは電子マネーの残高変更処理等を行なう、具体的な一例としては、チケット換金サーバ６５０は各エンティティの銀行口座を管理する銀行内のサーバとする設定が可能である。

【０２２３】チケット換金サーバ６５０は、コンテンツ取り引きに伴う発行チケットに基づく換金処理の管理データを管理するチケット換金管理データベース６５２を有する。さらに、各エンティテイからの受信チケット検証、チケット換金管理データベースの制御、各エンティテイとの通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６５３を有する。

【０２２４】チケット換金管理データベース６５２のデータ構成を図４５に示す。チケット換金管理データベー

ス６５２は、チケット換金サーバが受領チケットに応じてチケット換金処理を実行する際に内部生成する識別番号としてのチケット換金サーバ処理Ｎｏ．、チケットに基づく換金の要求を行なってきた要求主体識別子としての換金依頼元ＩＤ、コンテンツ取り引きに伴いチケットを発行するチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、チケットに基づく換金金額、コンテンツの購入主体であるユーザ機器の識別子としてのユーザ機器ＩＤ、コンテンツ取り引きを実行する際に、ユーザ機器で生成発行するトランザクションＩＤ、さらに、チケット換金サーバにおける換金処理のステータスを示すステータスの各情報を持つ。ステータスは、後段で詳細に説明するがコンテンツの取り引きに伴う複数の処理の進行に応じて更新される。

【０２２５】さらに、チケット換金サーバ６５０は、チケット換金管理データベース６５２のデータ生成、更新処理、受領チケットの検証処理、各種エンティテイとの通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段６５３を有する。制御手段６５３は、図４４に示すように暗号処理手段、通信処理手段としての機能も有し、制御手段６５３は、例えば暗号処理プログラム、通信処理プログラムを格納したコンピュータによって構成される。制御手段６５３の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。チケット換金サーバ６５０が格納する暗号鍵等の暗号処理用データとしては、チケット換金サーバ６５０の秘密鍵：ＫｓＴＥＳ、チケット換金サーバ６５０の公開鍵証明書Ｃｅｒｔ＿ＴＥＳ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２２６】制御手段６５３の構成は、先に図４を用いて説明した制御手段構成と同様の構成、すなわち、中央演算処理装置（ＣＰＵ:Central Processing Unit）、ＲＯＭ（Read only Memory）、ＲＡＭ（Random Access Memory）、表示部、入力部、記憶手段、通信インタフェース等を持つ構成である。

【０２２７】［コンテンツ購入処理］次に、図３７に戻り、ユーザ機器が、チケット発行サーバにコンテンツ購入要求を発行してコンテンツを利用可能な状態としてユーザ機器に保存し、チケットに基づいてコンテンツ料金が配分（換金）されるまでの処理について説明する。図３７の番号（１）から（３２）の順に処理が進行する。各番号順に処理の詳細を説明する。

【０２２８】（１）相互認証

コンテンツを購入しようとするユーザ機器６２０は、チケット発行サーバ６１０との間で相互認証処理を行なう。相互認証処理は、図１２または図１３を用いて説明した処理である。相互認証処理において、生成したセッション鍵を用いて、必要に応じて送信データを暗号化してデータ通信を実行する。

【０２２９】（２）トランザクションＩＤ、購入要求データ生成、および

（３）購入要求データ送信

チケット発行サーバ６１０とユーザ機器６２０間の相互認証が成功すると、ユーザ機器６２０は、コンテンツの購入要求データを生成する。購入要求データの構成を図４６（ｍ）に示す。購入要求データは、コンテンツ購入の要求元であるユーザ機器６２０の識別子である機器ＩＤ、取り引きの識別子として、ユーザ機器６２０の暗号処理手段が例えば乱数に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤの各データを有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、購入要求データには、署名検証用に必要に応じてユーザ機器の公開鍵証明書を添付する。

【０２３０】（４）受信データ検証

図４６（ｍ）に示す購入要求データをユーザ機器６２０から受信したチケット発行サーバ６１０は、受信データの検証処理を実行する。検証処理の詳細は、先に図１５を用いて説明した通りである。

【０２３１】（５）課金処理

（６）電子チケット発行

（７）電子チケット送信

チケット発行サーバ６１０は、次に、コンテンツの取り引きに関する課金処理、電子チケット発行処理を実行する。これらの処理は、例えば予め登録されているユーザ口座、あるいは電子マネー口座等に基づいて設定されるユーザの取り引き金額限度内の電子チケットを発行する処理として実行される。発行された電子チケットは、ユーザ機器６２０に送信される。

【０２３２】電子チケットの構成例を図４７に示す。図４７（Ａ）は、電子チケットに基づく料金配分先（料金受領エンティテイ）が単一である場合のデータ構成であり、チケット発行体ＩＤ、チケット発行処理Ｎｏ．、電子チケットに基づく料金配分先（エンティテイ）を示すチケット利用先ＩＤ、電子チケットに基づいて配分される料金を示す金額、電子チケットの有効期限、すなわち料金受領エンティテイがチケットに基づく換金（料金精算）処理を実行可能な期限、さらに、ユーザ機器からチケット発行サーバに対して送信された購入要求データ（図４６（ｍ）参照）を含む。なお、さらに、チケット発行日等のデータを付加してもよい。これらのデータにチケット発行サーバ６１０の電子署名が付加される。さらに、電子チケットには、署名検証用に必要に応じてチケット発行サーバの公開鍵証明書を添付する。

【０２３３】図４７（Ｂ）は、電子チケットに基づく料金配分先（エンティテイ）が複数である場合のデータ構

成であり、チケット利用先ＩＤが複数（１～ｎ）格納され、それぞれのチケット利用先ＩＤ毎に、電子チケットに基づいて配分される料金を示す金額が１～ｎまで格納されている。チケットに基づいて料金を受領するエンティティは、自己のＩＤに対応する金額を受領する。

【０２３４】図３７の処理例では、チケット発行サーバ６１０は、配信サーバを管理するコンテンツプロバイダ（ＣＰ）用の電子チケットと、ユーザ機器認証サーバ（ＤＡＳ）用の電子チケットを発行する。これらのチケット発行先は、コンテンツ毎に異なり、コンテンツの著作者等が含まれる場合もある。チケット発行サーバは、コンテンツＩＤに基づいてチケット発行先と、配分金額を定めたテーブルを有し、ユーザ機器からのコンテンツ購入要求に含まれるコンテンツＩＤに基づいてテーブルからチケット発行先と、配分金額データを取得してチケットを生成して発行する。

【０２３５】（８）受信データ検証

チケット発行サーバ６１０からチケットを受信したユーザ機器６２０は、チケットの検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器６２０は、まずチケット発行サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したチケット発行サーバの公開鍵ＫｐＴＩＳを用いてチケットの署名検証を実行する。

【０２３６】（９）相互認証

（１０）電子チケット（ＣＰ用）送信

次にユーザ機器６２０は、配信サーバ６４０にアクセスし、相互認証処理を実行する。相互認証が成立すると、ユーザ機器６２０は、配信サーバ６４０に対して、配信サーバ用の電子チケット（ＣＰ用）を送信する。

【０２３７】（１１）受信データ検証

（１２）暗号化コンテンツおよび暗号化コンテンツ鍵送信

配信サーバ６４０において、電子チケット（ＣＰ用）の検証が完了し、データ改竄のない正当な電子チケットであると判定すると、配信サーバ６４０は、暗号化コンテンツおよび暗号化コンテンツ鍵をユーザ機器に送信する。これらは、コンテンツをコンテンツキーで暗号化した暗号化コンテンツ：Ｋｃ（content）と、コンテンツキー：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）６３０の公開鍵で暗号化した暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を含むデータである。

【０２３８】（１３）受信データ検証

（１４）相互認証

（１５）電子チケット（ＤＡＳ用）および鍵かけかえ要求送信

配信サーバ６４０から暗号化コンテンツおよび暗号化コンテンツ鍵を受信したユーザ機器６２０は、データの検証処理を実行する。データ検証後、ユーザ機器６２０は、ユーザ機器認証サーバ６３０にアクセスし、相互認証処理を実行する。相互認証が成立すると、ユーザ機器６２０は、ユーザ機器認証サーバ６３０に対して、ユーザ機器認証サーバ用の電子チケット（ＤＡＳ）および鍵かけかえ要求を送信する。鍵かけかえ要求は、先に配信サーバ６４０から受信したユーザ機器認証サーバの公開鍵で暗号化されたコンテンツ鍵Ｋｃである。暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）をユーザ機器の公開鍵ＫｐＤＥＶで暗号化したコンテンツ鍵、すなわちＫｐＤＥＶ（Ｋｃ）とする処理を要求するものであり、図１を用いて説明したかけかえ処理と同様である。

【０２３９】（１６）受信データ検証

（１７）暗号化コンテンツ鍵かけかえ処理、ユーザ機器６２０から電子チケット（ＤＡＳ用）および暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）かけかえ要求を受信したユーザ機器認証サーバ６３０は、電子チケット（ＤＡＳ用）、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。検証が終了し、データの改竄のない正当な電子チケットであり、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ６３０は、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）６３０の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ６３０の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。この処理は、前述の図１６を用いて説明した処理と同様である。

【０２４０】（１８）暗号化コンテンツ鍵送信

（１９）受信データ検証

（２０）保存処理

ユーザ機器認証サーバ６３０は、鍵かけかえにより生成した暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）をユーザ機器６２０に送信する。ユーザ機器認証サーバ６３０から、暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を受領したユーザ機器６２０は、受信データ検証処理を実行し、検証後、ユーザ機器６２０は、暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器６２０の記憶手段に格納する。コンテンツの利用時には、暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０２４１】（２１）相互認証

（２２）電子チケット（ＣＰ用）送信

配信サーバ６４０は、ユーザ機器６２０に対する暗号化

コンテンツ配信の後、チケット換金サーバ６５０にアクセスし、相互認証処理を実行する。相互認証が成立すると、配信サーバ６４０は、チケット換金サーバ６５０に対して、配信サーバ用の電子チケット（ＣＰ用）を送信する。

【０２４２】（２３）受信データ検証、換金処理

チケット換金サーバ６５０において、電子チケット（ＣＰ用）の検証が完了し、データ改竄のない正当な電子チケットであると判定すると、チケット換金サーバ６５０は、受領した電子チケット（ＣＰ用）に基づいて換金処理を実行する。換金処理は、例えば予め登録されている配信サーバを管理するコンテンツプロバイダ（ＣＰ）の管理口座、あるいは電子マネー口座等に、電子チケット（ＣＰ用）に設定された金額をユーザ機器の管理ユーザの口座から振り替える処理として行われる。あるいは既にチケット発行サーバがユーザからの前払い預り金として受領しているチケット発行サーバ管理口座からコンテンツプロバイダ（ＣＰ）の管理口座にチケットに設定された金額を振り替える処理として行なってもよい。なお、チケット換金サーバ６５０は、チケットに格納された有効期限を検証し、有効期限内であることが確認されたことを条件として該チケットに基づく料金精算処理を実行する。

【０２４３】（２４）換金処理レポート報告

チケット換金サーバ６５０において、電子チケット（ＣＰ用）に基づく換金が終了すると、チケット換金サーバ６５０は、配信サーバ６４０に対して換金処理が済んだことを示すレポートを送信する。

【０２４４】換金処理レポートの構成例を図４６（ｎ）に示す。換金処理レポートは、チケット換金処理個々の識別子であるチケット換金処理ＩＤ、チケットに基づく換金の要求を行なってきた要求主体識別子としての換金依頼元ＩＤ、チケットに基づく換金金額、コンテンツ取り引きに伴いチケットを発行したチケット発行体の識別子であるチケット発行体ＩＤ、チケット発行サーバ６１０が設定するチケット発行処理Ｎｏ．、チケット換金サーバ６５０において換金処理が実行されたチケット換金処理完了日等のデータを有し、これらにチケット換金サーバ６５０の電子署名が付加される。さらに、換金処理レポートには、署名検証用に必要に応じてチケット換金サーバの公開鍵証明書を添付する。

【０２４５】（２５）受信データ検証

チケット換金サーバ６５０から換金処理レポートを受信した配信サーバ６４０は、換金処理レポートの検証処理を実行する。データ検証により、レポートが正当であると認められれば、配信サーバの管理主体であるコンテンツプロバイダに対するコンテンツ取り引きに伴う料金配分が完了したことが確認される。

【０２４６】（２６）相互認証

（２７）電子チケット（ＤＡＳ用）送信

（２８）受信データ検証、換金処理

（２９）換金処理レポート報告

（３０）受信データ検証

ユーザ機器認証サーバ６３０とチケット換金サーバ６５０との間においても、上述の配信サーバ６４０とチケット換金サーバ６５０間の処理（２１）～（２５）と同様の処理が電子チケット（ＤＡＳ用）に基づいて実行される。

【０２４７】（３１）相互認証

（３２）換金処理レポート報告

（３３）受信データ検証

また、チケット換金サーバ６５０は、各エンティテイから受領したチケットに基づいて換金処理を実行した場合、チケット発行サーバ６１０との相互認証後、各エンティテイに送付したと同様の換金処理レポート（図４６（ｎ）参照）をチケット発行サーバ６１０に送信する。チケット発行サーバ６１０は、チケット換金サーバ６５０から受信した換金処理レポートの検証を実行し、発行したチケットに関する換金処理が完了したことを確認する。

【０２４８】（各機器におけるステータス遷移）図３７に示すチケット発行サーバ６１０等の各エンティテイは、それぞれコンテンツ取り引きに係る一連の処理において、処理状態を示すステータスに応じて、次の処理を決定する。ステータスは、例えば図３９に示すチケット発行管理データベース、図４０のユーザ機器の購入管理データベース等において、各コンテンツ取り引き毎に管理される。

【０２４９】まず、チケット発行サーバ６１０のステータス遷移について、図４８を用いて説明する。チケット発行サーバ６１０は、ユーザ機器６２０からのコンテンツ購入要求データを受信（図３７の処理（３）に対応）することで処理が開始される。チケット発行サーバ６１０は、ユーザ機器６２０からの受信データを検証し、検証に成功した場合は、ステータスを「購入受付完了」に設定し、データ検証により正当な購入要求であるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、購入受付処理を所定回数繰り返した後処理を中止し、ステータスを「購入受付失敗」とする。ステータスが「購入受付完了」である場合にのみ次ステップに進む。

【０２５０】ステータスが「購入受付完了」に遷移すると、次に、チケット発行サーバ６１０は、ユーザ機器６２０に対して電子チケットを送信（図３７の処理（７）に対応）し、ユーザ機器からの受信応答（レスポンス）を受領することにより、ステータスを「チケット配信完了」とする。受信応答（レスポンス）を受領しなかった場合は、処理を中止するか、あるいは同様の処理、ここでは、電子チケットの送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット配信失敗」

とする。ステータスが「チケット配信完了」である場合にのみ次ステップに進む。

【０２５１】ステータスが「チケット配信完了」に遷移した場合、次に、チケット発行サーバ６１０は、チケット換金サーバから換金処理レポートを受信し、レポートの検証（図３７の処理（３２）、（３３）に対応）を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。チケット発行サーバ６１０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２５２】次にユーザ機器認証サーバ６３０のステータス遷移について、図４９を用いて説明する。ユーザ機器認証サーバ６３０は、ユーザ機器６２０からの暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を受信（図３７の処理（１５）に対応）することで処理が開始される。ユーザ機器認証サーバ６３０は、ユーザ機器６２０からの電子チケット（ＤＡＳ）を含む受信データを検証し、検証に成功した場合は、ステータスを「鍵受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ユーザ機器）の受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵受信失敗」とする。ステータスが「鍵受信完了」である場合にのみ次ステップに進む。

【０２５３】ステータスが「鍵受信完了」に遷移すると、次に、ユーザ機器認証サーバ６３０は、コンテンツ鍵かけかえ処理（図３７の処理（１７）に対応）を実行し、鍵かけかえ処理が成功した場合には、ステータスを「鍵かけかえ完了」とする。鍵かけかえに失敗することは想定していないので、ここでは「鍵かけかえ完了」のみのステータス遷移が存在する。

【０２５４】ステータスが「鍵かけかえ完了」に遷移した場合、次に、ユーザ機器認証サーバ６３０は、ユーザ機器６２０に対して暗号化コンテンツ鍵データ（ＤＡＳ）を送信（図３７の処理（１８）に対応）し、ユーザ機器６２０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「鍵送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツ鍵データ（ＤＡＳ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵送信失敗」とする。

【０２５５】ステータスが「鍵送信完了」に遷移すると、次に、ユーザ機器認証サーバ６３０は、チケット換金サーバ６５０に対して、電子チケット（ＤＡＳ用）を送信（図３７の処理（２７）に対応）し、チケット換金サーバ６５０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「チケット換金要求送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット換金要求の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット換金要求失敗」とする。

【０２５６】ステータスが「チケット換金要求送信完了」に遷移すると、次に、ユーザ機器認証サーバ６３０は、チケット換金サーバ６５０からの換金処理レポートを受信し、レポートの検証処理（図３７の処理（２９）、（３０）に対応）を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。ユーザ機器認証サーバ６３０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２５７】次に配信サーバ６４０のステータス遷移について、図５０を用いて説明する。配信サーバ６４０は、ユーザ機器６２０からの電子チケット（ＣＰ用）を受信（図３７の処理（１０）に対応）することで処理が開始される。配信サーバ６４０は、ユーザ機器６２０からの受信データを検証し、検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケットの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【０２５８】ステータスが「電子チケット受信完了」に遷移すると、次に、配信サーバ６４０は、ユーザ機器６２０に対して暗号化コンテンツおよび暗号化コンテンツ鍵データＫｐＤＡＳ（Ｋｃ）を送信（図３７の処理（１２）に対応）し、ユーザ機器６２０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「配信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、暗号化コンテンツおよび暗号化コンテンツ鍵データＫｐＤＡＳ（Ｋｃ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「配信失敗」とする。

【０２５９】ステータスが「配信完了」に遷移すると、次に、配信サーバ６４０は、チケット換金サーバ６５０に対して、電子チケット（ＣＰ用）を送信（図３７の処

理（２２）に対応）し、チケット換金サーバ６５０からのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「チケット換金要求送信完了」に設定し、データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット換金要求の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「チケット換金要求失敗」とする。

【０２６０】ステータスが「チケット換金要求送信完了」に遷移すると、次に、配信サーバ６４０は、チケット換金サーバ６５０からの換金処理レポートを受信し、レポートの検証処理（図３７の処理（２４）、（２５）に対応）を実行する。検証に成功した場合は、ステータスを「換金処理レポート受信完了」に設定し、処理終了とする。レポート検証により正当なレポートであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、レポート受信、検証処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート受信失敗」とする。配信サーバ６４０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２６１】次に、ユーザ機器６２０のステータス遷移について、図５１を用いて説明する。ユーザ機器６２０は、まず、チケット発行サーバ６１０に対して購入要求データを送信（図３７の処理（３）に対応）することで処理が開始される。ユーザ機器６２０は、チケット発行サーバ６１０に対する購入要求データの受信完了のレスポンスを受信すると、ステータスを「購入要求送信完了」に設定し、チケット発行サーバ６１０からの受信完了のレスポンスを受信できない場合は、処理を中止するか、あるいは同様の処理、ここでは、購入要求送信処理を所定回数繰り返した後、処理を中止し、ステータスを「購入要求送信失敗」とする。ステータスが「購入要求送信完了」である場合にのみ次ステップに進む。

【０２６２】ステータスが「購入要求送信完了」に遷移すると、次に、ユーザ機器６２０は、チケット発行サーバ６１０から、電子チケットを受信（図３７の処理（７）、（８）に対応）し、受信データを検証する。チケット発行サーバ６１０からのチケットの検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なチケットであるとの判定がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、チケット受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【０２６３】ステータスが「電子チケット受信完了」に遷移した場合、次に、ユーザ機器６２０は、配信サーバ６４０に対して、電子チケットを送信（図３７の処理（１０）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「電子チケット送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、チケット送信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット送信失敗」とする。ステータスが「電子チケット送信完了」である場合にのみ次ステップに進む。

【０２６４】ステータスが「電子チケット送信完了」に遷移すると、次に、ユーザ機器６２０は、配信サーバ６４０から、暗号化コンテンツと、暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を受信し、データ検証（図３７の処理（１２）、（１３）に対応）を実行する。データ検証に成功した場合は、ステータスを「鍵１受信完了」に設定し、データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵１受信失敗」とする。

【０２６５】ステータスが「鍵１受信完了」に遷移すると、次に、ユーザ機器６２０は、ユーザ機器認証サーバ６３０に対して電子チケット（ＤＡＳ用）と暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を送信（図３７の処理（１５）に対応）し、データ受信レスポンスを受信する。データ受信レスポンスを受信した場合は、ステータスを「鍵かけかえ要求送信完了」に設定し、データ受信レスポンスを受信しない場合は、処理を中止するか、あるいは同様の処理、ここでは、電子チケット（ＤＡＳ用）と暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）の送信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵かけかえ要求送信失敗」とする。ステータスが「鍵かけかえ要求送信完了」である場合にのみ次ステップに進む。

【０２６６】ステータスが「鍵かけかえ要求送信完了」に遷移すると、次に、ユーザ機器６２０は、ユーザ機器認証サーバ６３０から、暗号化コンテンツ鍵ＫｐＤＥＶ（Ｋｃ）を受信し、データ検証（図３７の処理（１８）、（１９）に対応）を実行する。データ検証に成功した場合は、ステータスを「鍵２受信完了」に設定し、処理を終了する。データ検証に成功しなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、鍵データの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「鍵２受信失敗」とする。

【０２６７】次にチケット換金サーバ６５０のステータス遷移について、図５２を用いて説明する。チケット換金サーバ６５０は、電子チケットによる配分権を持つエンティテイからの電子チケットを受信（図３７の処理（２２）、（２７）に対応）することで処理が開始される。チケット換金サーバ６５０は、受信チケットを検証し、検証に成功した場合は、ステータスを「電子チケット受信完了」に設定し、データ検証により正当なデータであるとの判定がなされなかった場合等には、処理を中

止するか、あるいは同様の処理、ここでは、チケットの受信処理を所定回数繰り返した後、処理を中止し、ステータスを「電子チケット受信失敗」とする。ステータスが「電子チケット受信完了」である場合にのみ次ステップに進む。

【０２６８】ステータスが「電子チケット受信完了」に遷移すると、次に、チケット換金サーバ６５０は、電子チケットに基づく換金処理を実行する。換金処理は、予め登録されている利益配分エンティテイ、例えば配信サーバを管理するコンテンツプロバイダ（ＣＰ）の管理口座、あるいは電子マネー口座等に、電子チケット（ＣＰ用）に設定された金額をユーザ機器の管理ユーザの口座から振り替える処理、あるいは既にチケット発行サーバがユーザからの前払い預り金として受領しているチケット発行サーバ管理口座からコンテンツプロバイダ（ＣＰ）の管理口座にチケットに設定された金額を振り替える処理として行なわれる。換金処理が完了するとステータスを「換金処理完了」に設定し、換金処理が実行できなかった場合には、処理を中止し、ステータスを「換金処理失敗」とする。

【０２６９】ステータスが「換金処理完了」に遷移すると、次に、チケット換金サーバ６５０は、チケットを送信してきたエンティテイに対して、換金処理レポートを送信（図３７の処理（２４）、（２９）に対応）し、各エンティテイからのデータ受信応答を受信する。データ受信応答を受信した場合は、ステータスを「換金レポート送信完了」に設定し、処理を終了する。データ受信応答の受信がなされなかった場合等には、処理を中止するか、あるいは同様の処理、ここでは、換金レポートの送信処理を所定回数繰り返した後、処理を中止し、ステータスを「換金レポート送信失敗」とする。チケット換金サーバ６５０は、このような状態遷移を各コンテンツ取り引き毎に実行する。

【０２７０】図５３にチケット発行体によって発行されるチケットを流通させることによりコンテンツ料金の精算処理を行なう具体的構成例を示す。ユーザ機器８０２からチケット発行体８０１に対してコンテンツ購入要求があると、チケット発行体は、コンテンツの取り引きに関する課金処理、電子チケット発行処理を実行する。これらの処理は、例えば予め登録されているユーザ口座、あるいは電子マネー口座等に基づいて設定されるユーザの取り引き金額限度内の電子チケットを発行する処理として実行される。図５３に示す例では、コンテンツ購入代金として１，０００円分の電子チケットをチケット発行体がユーザ機器に対して発行する。

【０２７１】図５３の例では、コンテンツ料金１０００円の配分は、図上部に示すように、チケット発行体としてのショップが販売手数料としてのショップ利益として３００円、コンテンツ配信のシステム運営者であるライセンスホルダ（ユーザ機器認証サーバ）８０３がライセンス料として１００円、コンテンツ製作者（配信サーバ）がコンテンツ料として６００円を、それぞれ受領する設定であるとする。

【０２７２】ユーザ機器からの購入要求を受領したチケット発行体８０１は、コンテンツＩＤからコンテンツ料金の配分比率の設定情報を求め、複数の料金配分先がある場合は、それぞれの電子チケットを発行する。図５３の例では、ライセンスホルダ８０３に対するセイセンス料、１００円の配分料金を設定した電子チケットと、コンテンツ製作者に対するコンテンツ料、６００円のチケットをユーザ機器８０２に配信する。配信する電子チケットには、チケット発行体の署名が生成される。

【０２７３】ユーザ機器８０２は、ライセンスホルダ８０３、コンテンツ製作者８０４それぞれに各電子チケットを送信する。ライセンスホルダ８０３、コンテンツ製作者８０４は、受領した電子チケットを検証して、正当なチケットであることを確認した後、銀行（チケット換金サーバ）８０５にチケットを送信し、換金サーバにおいても署名検証を実行し、正当なチケットであることを確認してそれぞれの配分料金の換金（ｅｘ．振替処理）を行なう。なお、銀行（チケット換金サーバ）において実行するチケットの署名検証は、電子チケットに対して生成されたチケット発行体の署名の検証である。また、チケットに含まれる購入要求データのユーザ機器署名の検証も実行する。

【０２７４】さらに、チケットの送信主体であるコンテンツ製作者、ライセンスホルダが電子チケットを含む送信データに対して署名を生成し、これらの署名についても銀行（チケット換金サーバ）が署名検証を実行する構成としてもよい。

【０２７５】図５３の構成では、チケット発行体（ショップ）８０１自身もコンテンツ料金の一部３００円分の自己の電子チケットを銀行（チケット換金サーバ）８０５に送付して換金を行なう構成である。

【０２７６】これらの各電子チケットの換金処理により、確実にコンテンツ料金の配分が実行される。コンテンツ製作者８０４は、電子チケットをユーザ機器８０２から受領して検証した後、コンテンツ鍵Ｋｃで暗号化した暗号化コンテンツと、コンテンツ鍵Ｋｃをライセンスホルダ（ユーザ機器認証サーバ）の公開鍵ＫｐＤＡＳで暗号化した暗号化コンテンツ鍵：ＫｐＤＡＳ（Ｋｃ）をユーザ機器８０２に送信する。

【０２７７】ユーザ機器８０２は、コンテンツ制作者８０４から受領した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）を電子チケット（ＤＡＳ）とともに、ライセンスホルダ８０３に送信する。ライセンスホルダは、電子チケットの検証の後、暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）の鍵かけかえ処理を実行し、ユーザ機器の公開鍵ＫｐＤＥＶでコンテンツ鍵を暗号化して、ＫｐＤＥＶ（Ｋｃ）を生成してユーザ機器８０２に送信する。ユーザ機

器８０２は、ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶで復号してコンテンツ鍵Ｋｃを得ることができる。またコンテンツ鍵をデバイスに格納する場合は、自己の保存鍵Ｋｓｔｏで暗号化して保存する。

【０２７８】上述したように、チケット発行体によって発行するチケットを受信し、正当なチケットであることを条件として配信サーバ（ｅｘ．コンテンツ製作者）が暗号化コンテンツと暗号化コンテンツ鍵をユーザ機器に送信し、一方、ライセンスホルダ（ユーザ認証機器）が、同様に電子チケットを受領し、正当なチケットであることを条件として暗号化コンテンツ鍵のかけかえを行なってユーザ機器に配信する構成としたことにより、電子チケットに基づく確実なコンテンツ料金の配分が実行され、ユーザ機器においてコンテンツの利用が可能となる。

【０２７９】［３．ログ収集サーバによるコンテンツ配信管理］次に、ユーザ機器がコンテンツの購入を行なった事実をユーザ機器にログとして蓄積し、ログの回収をシステム運営者が行なうことにより、コンテンツの流通実体を正確に把握可能としたコンテンツ配信システムについて説明する。

【０２８０】図５４にログ回収システムを持つコンテンツ配信形態のシステム構成を示す。図５４のコンテンツ配信システムは、ユーザ機器に対するコンテンツの配信サービスを行なうショップサーバ（ＳＨＯＰ）９０１、ショップサーバ９０１からのコンテンツ配信を受信するユーザ機器（ＤＥＶＩＣＥ）９０２、さらに、正当なコンテンツ取り引き管理のためのログ管理サーバとして機能するログ収集サーバ９０３を主構成要素とし、コンテンツの提供者としてのコンテンツプロバイダ９０５と、コンテンツプロバイダ９０５から提供されるコンテンツに対してコンテンツの利用制限情報等の各種情報をヘッダとして生成し、ショップサーバに提供するオーサリングサーバ９０４、さらに、各エンティテイに対して公開鍵証明書（Ｃｅｒｔ＿ｘｘｘ）を発行する認証局（ＣＡ：Certificate Authority）を有する。

【０２８１】図５４の構成において、コンテンツプロバイダ９０５とオーサリングサーバ９０４は、ショップサーバ９０１に対して、流通対象となるコンテンツを提供するエンティテイ構成の一例であり、図５４の形態に限らず、他の様々な態様でショップサーバに対する流通コンテンツの提供がなされる。例えばコンテンツプロバイダから直接ショップサーバにコンテンツが提供されてもよいし、コンテンツの保持者である著作者から複数のサービスプロバイダを介してショップサーバにコンテンツが提供される場合もある。

【０２８２】図５４の構成例は、本発明の説明の理解を容易にするために、コンテンツ売り上げの一部を取得する権利を持つエンティテイの1つの代表例としてコンテンツプロバイダ９０５を示したものである。図５４の構成例では、コンテンツプロバイダ９０５は、ログ収集サーバ９０３によって収集されるログに基づいて管理されるコンテンツ売り上げデータの確認により、自己の配分利益を確実に取得することができる。他の利益配分権を有するエンティテイがある場合は、そのエンティテイが図５４の構成に加わり、ログ収集サーバ９０３によって収集されるログに基づいて自己の配分利益を確認可能である。

【０２８３】図５４の構成において、ショップサーバ９０１は、図１他の構成において説明したと同様の構成であり、暗号処理、通信処理可能な制御部を有し、コンテンツ取り引き処理に伴うステータス管理を実行して、各機器における取り引き処理シーケンスを実行する。また、コンテンツプロバイダ９０５とオーサリングサーバ９０４も暗号処理、通信処理可能な制御部を有し、コンテンツ取り引き処理に伴うステータス管理を実行して、各機器における取り引き処理シーケンスを実行する。

【０２８４】（ユーザ機器）ユーザ機器９０２は、先に図７を用いて説明した構成と同様であり、暗号処理、通信処理可能な制御手段２３０（図７参照）を有する。ただし、本実施例では、制御手段２３０は、コンテンツ購入処理毎にログデータを生成し、購入管理データベース２２０中に生成したログデータを格納する。

【０２８５】ユーザ機器９０２において生成され格納されるログデータの構成例を図５５に示す。図５５には、ログデータの例を２つ示している。（Ａ）構成例１は、ユーザ機器９０２がショップサーバ９０１との取り引きにより取得したコンテンツの識別子であるコンテンツＩＤ、ユーザ機器の識別子であるユーザ機器ＩＤ（ＩＤ＿ＤＥＶ）、取り引きを行なったショップの識別子であるショップＩＤ（ＩＤ＿ＳＨＯＰ）、取り引きの日時を示す日付情報が含まれ、これらのデータに対するユーザ機器の署名（Ｓｉｇ．ＤＥＶ）が生成されている。ログ収集サーバはユーザ機器から受信する購入ログの電子署名の検証処理を実行する。（Ｂ）構成例２は、販売確認データとコンテンツの受領日時データに対してユーザ機器の署名（Ｓｉｇ．ＤＥＶ）が生成された構成である。販売確認データは、ショップサーバ９０１がユーザ機器９０２からのコンテンツ購入要求に基づいて生成するコンテンツの販売を実行したことを示すデータである。販売確認データについては、後段でさらに説明する。

【０２８６】ユーザ機器９０２は、コンテンツ購入処理に際して、例えば図５５に示すログデータを生成しユーザ機器内に格納する。格納されたログデータは、ログ収集サーバ９０３に送信される。ユーザ機器は自己の公開鍵証明書の更新処理実行時に、その間に蓄積したログデータをログ収集サーバ９０３に送信する。これらの処理シーケンスについては、フローを用いて後段で詳細に説明する。

【０２８７】（ログ収集サーバ）ログ収集サーバ９０３

は、図５６に示す構成を有する。ログ収集サーバは、収集ログ管理データベース９０３１を有する。収集ログ管理データベース９０３１は、様々なユーザ機器から受領するログデータ（図５５参照）を格納するデータベースである。

【０２８８】ログ収集サーバ９０３は、ユーザ機器９０２、ショップサーバ９０１等との通信処理、さらに、各通信処理に際してのデータ暗号処理等を実行する制御手段９０３２を有する。制御手段９０３２は、先に説明したショップサーバ等の制御手段と同様、暗号処理手段、通信処理手段としての機能も有する。その構成は、図４を用いて説明した構成と同様である。制御手段９０３２の暗号処理手段において実行される暗号処理において使用される鍵データ等は、制御手段内部の記憶手段にセキュアに格納されている。ログ収集サーバ９０３が格納する暗号鍵等の暗号処理用データとしては、ログ収集サーバ９０３の秘密鍵：ＫｓＬＯＧ、ログ収集サーバ９０３の公開鍵証明書Ｃｅｒｔ＿ＬＯＧ、公開鍵証明書の発行機関である公開鍵証明書発行局としての認証局（ＣＡ：Certificate Authority）の公開鍵ＫｐＣＡがある。

【０２８９】ログ収集サーバ９０３は、ユーザ機器９０２からのログデータ受領と引き換えに、公開鍵証明書の発行手続き処理を実行する。具体的には、ユーザ機器９０２から更新用の公開鍵を受領して、受領した公開鍵を認証局９０６に転送して、ユーザ機器の公開鍵証明書の発行要求を行ない、認証局９０６の発行した公開鍵証明書を受領してユーザ機器９０２に送信する。この一連の処理については、フローを用いて後段で詳細に説明する。

【０２９０】（コンテンツ購入処理）本実施例における処理は、図５４の上段に示すように、

Ａ．コンテンツ購入処理

Ｂ．ログ送信、公開鍵証明書更新処理

Ｃ．コンテンツ販売準備処理

Ｄ．売り上げ確認処理

の４つの処理に分類される。以下、これらの各処理についてフローを用いて説明する。

【０２９１】（Ａ．コンテンツ購入処理）コンテンツ購入処理について、図５７、図５８のフローを用いて説明する。図５７、図５８においては、左側にユーザ機器、右側にショップサーバの処理を示している。まず、図５７に示すように、処理開始時に、ユーザ機器とショップサーバ間において相互認証が実行される（Ｓ１５０１，Ｓ１６０１）。

【０２９２】相互認証処理は、図１３を用いて説明した公開鍵方式に基づく処理として実行される。この相互認証においては、認証局（ＣＡ）９０６の発行する有効期限の設定された公開鍵証明書を用いて行われ、ユーザ機器は、有効期限内の公開鍵証明書を持つことが相互認証を成立させるための条件として求められる。後段で説明するが、公開鍵証明書の更新処理は、ログ収集サーバ９０３に対するログの送信を条件として実行される。

【０２９３】相互認証処理において生成したセッション鍵（Ｋｓｅｓ）は、必要に応じて送信データを暗号化してデータ通信を実行したり、あるいはＫｓｅｓを用いた改竄チェック値（ＩＣＶ：Integrity Check Value）の生成処理に使用される。ＩＣＶの生成については後述する。

【０２９４】相互認証が成立すると、ユーザ機器は、コンテンツ取り引きにおいて適用するトランザクションＩＤを例えば乱数に基づいて生成し、購入要求データを生成（Ｓ１５０２）する。購入要求データのフォーマット例を図５９（Ａ）に示す。

【０２９５】購入要求データには前述のトランザクションＩＤ（ＴＩＤ＿ＤＥＶ）、コンテンツ識別子であるコンテンツＩＤ、ユーザ機器の識別子であるユーザ機器ＩＤ（ＩＤ＿ＤＥＶ）、コンテンツ価格である表示価格、さらに購入依頼日時を含み、これらのデータに対するユーザ機器の署名（Ｓｉｇ．Ｄｅｖ）を生成した構成である。

【０２９６】さらに、ユーザ機器は、購入要求データの改竄チェック値（ＩＣＶ１）を生成して、ショップサーバに送信（Ｓ１５０３）する。改竄チェック値（ＩＣＶ）は、改竄チェック対象データに対するハッシュ関数を用いて計算され、ＩＣＶ＝ｈａｓｈ（Ｋｉｃｖ，Ｃ１，Ｃ２，…）によって計算される。ＫｉｃｖはＩＣＶ生成キーである。Ｃ１，Ｃ２は改竄チェック対象データの情報であり、改竄チェック対象データの重要情報のメッセージ認証符号（ＭＡＣ：Message authentication Code）が使用される。

【０２９７】ＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図６０に示す。図６０の構成に示すように対象となるメッセージを８バイト単位に分割し、（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）、まず、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮがメッセージ認証符号（ＭＡＣ（Message Authentication Code））となる。なお、メッセージとしては、検証対象となるデータを構成する部分データが使用可能である。

【０２９８】このようなチェック対象データの改竄チェック値（ＩＣＶ）は、ＩＣＶ生成キーＫｉｃｖを用いて生成されたＭＡＣ値として構成される。改竄のないことが保証された例えばデータ送信側がデータ生成時に生成したＩＣＶと、データ受信側が受信データに基づいて生

成したＩＣＶとを比較して同一のＩＣＶが得られればデータに改竄のないことが保証され、ＩＣＶが異なれば、改竄があったと判定される。

【０２９９】ここでは、ＩＣＶ生成キーとして相互認証時に生成したセッション鍵：Ｋｓｅｓを使用する。ユーザ機器は、セッション鍵：Ｋｓｅｓを適用して購入要求データ（図５９（Ａ）参照）の改竄チェック値（ＩＣＶ１）を生成して、購入要求データ＋ＩＣＶ１をショップサーバに送信する。

【０３００】ショップサーバは、ＩＣＶ１の検証、すなわち、受信データに基づいてセッション鍵：Ｋｓｅｓを適用して改竄チェック値ＩＣＶ１’を生成して、受信したＩＣＶ１＝ＩＣＶ１’が成立するか否かを判定する。成立した場合は、改竄なしと判定する。さらに、ショップサーバは、購入要求データの署名検証（Ｓ１６０３）を行なう。署名検証は、ユーザ機器の公開鍵を用いて行なう。公開鍵はユーザ機器の公開鍵証明書Ｃｅｒｔ＿ＤＥＶから取り出されるものであり、有効期限内の公開鍵証明書であることが条件となる。有効期限の切れた公開鍵証明書は、ショップサーバにおいて署名検証に使用されず、購入依頼ＮＧとなる。ＩＣＶのチェック、署名検証いずれもＯＫであれば、ショップサーバは、販売確認データを生成（Ｓ１６０４）する。

【０３０１】販売確認データは、例えば図５９の（Ｂ）に示すデータ構成を持つ。ショップサーバの生成したトランザクションＩＤ（ＴＩＤ＿ＳＨＯＰ）、ショップの識別子であるショップＩＤ（ＩＤ＿ＳＨＯＰ）、販売日時、コンテンツ販売に対する運営者手数料情報、ここで運営者とは、例えば、コンテンツ販売システムの管理エンティテイ（ＳＨ：システムホルダ）であり、図５４では、ログ収集サーバ９０３を管理するエンティテイである。

【０３０２】さらに、ＣＰ（コンテンツプロバイダ）売り上げ分配情報、これは、コンテンツの売り上げに対するコンテンツプロバイダの配分を示す情報である。さらに、購入要求データ（図５９（Ａ）参照）を含み、これらのデータにショップの署名（Ｓｉｇ．ＳＨＯＰ）が生成された構成である。

【０３０３】図５９（Ｂ）の販売確認データフォーマットは、コンテンツの売り上げに対して運営者（ＳＨ：システムホルダ）と、コンテンツプロバイダ（ＣＰ）との２つのエンティテイの配分情報のみを記録しているが、この他にも、コンテンツ売り上げの配分先エンティテイが存在する場合は、それらの各エンティテイの配分情報も格納する。

【０３０４】ＩＣＶのチェック、署名検証いずれもＯＫであり、販売確認データを生成（Ｓ１６０４）すると、ショップサーバは購入を承諾するメッセージを含む購入ＯＫデータにセッション鍵Ｋｓｅｓを用いて改竄チェック値（ＩＣＶ２）を生成付加してユーザ機器に送信（Ｓ１６０５）する。ＩＣＶのチェック、署名検証いずれかがＮＧであると、ショップサーバは購入を拒否するメッセージを含む購入ＮＧデータにセッション鍵Ｋｓｅｓを用いて改竄チェック値（ＩＣＶ２）を生成付加してユーザ機器に送信（Ｓ１６０６）する。

【０３０５】さらに、ショップサーバは、購入ＯＫデータをユーザ機器に送信した場合は、販売確認データ（図５９（Ｂ）参照）と、ヘッダ（コンテンツの利用情報等を含む各種コンテンツ関連情報）に対してセッション鍵Ｋｓｅｓを用いて改竄チェック値（ＩＣＶ３）を生成したデータとコンテンツとをユーザ機器に送信（Ｓ１６０７）する。

【０３０６】ユーザ機器は、コンテンツおよび、購入要求応答データ（ＯＫまたはＮＧ）＋ＩＣＶ２を受信（Ｓ１５０４）し、ＩＣＶ２の検証を行ない、購入要求応答を確認（Ｓ１５０５）する。ＩＣＶ２によりデータ改竄なしと判定され、購入が受け入れられた（ＯＫ）であるときは、販売確認データ（図５９（Ｂ）参照）と、ヘッダ（コンテンツの利用情報等を含む各種コンテンツ関連情報）＋ＩＣＶ３を受信（Ｓ１５０６）し、ＩＣＶ３の検証、販売確認データの署名検証を行ないいずれもＯＫである場合は、コンテンツ受信ＯＫのレスポンスにＩＣＶ４を生成してショップサーバに送信する。

【０３０７】ステップＳ１５０７の判定がＮｏである場合は、ステップＳ１５０９において、コンテンツ受信ＮＧのレスポンスにＩＣＶ４を生成してショップサーバに送信する。

【０３０８】ショップサーバは、コンテンツ受信ＯＫまたはＮＧ＋ＩＣＶ４を受信（（Ｓ１６０８）し、ＩＣＶ４の検証を行ない（Ｓ１６１１）、さらにユーザ機器からの応答がコンテンツ受信ＯＫである場合は、ユーザに対するコンテンツの課金処理を実行（Ｓ１６１３）する。この課金処理は、前実施例と同様、例えば、ユーザの取り引き口座、あるいはクレジットカード指定口座からコンテンツ料金を受領する処理である。課金処理が終了すると、課金終了メッセージにＩＣＶ５を生成してユーザ機器に送信（Ｓ１６１４）する。ステップＳ１６１１、またはＳ１６１２の判定のいずれかがＮｏである場合は、ステップＳ１６１５において課金未了メッセージにＩＣＶ５を生成してユーザ機器に送信する。

【０３０９】課金終了（または未了）メッセージ＋ＩＣＶ５を受信したユーザ機器は、ＩＣＶ５の検証を実行し、さらに課金が無事終了したかを判定し、課金が済んだことを確認すると、購入ログ（図５５参照）を生成して自デバイスのメモリに保存の後、コンテンツの利用を行なう。ステップＳ１５１２、またはＳ１５１３の判定のいずれかがＮｏである場合は、ステップＳ１５１４においてショップサーバから受領したヘッダ、コンテンツを削除する処理を行なう。

【０３１０】次に、図６１、図６２を用いてユーザ機器

と、ログ収集サーバ間で行われる鍵更新処理と、ログ送信処理とについて説明する。図６１、図６２の左側にユーザ機器の処理、右側にログ収集サーバの処理を示す。この処理は、コンテンツをショップサーバから購入するユーザ機器がユーザ機器に格納されたユーザ機器の公開鍵証明書を更新する際に実行される。ユーザ機器の公開鍵証明書には有効期限が設定されており、一定期間毎に更新処理を実行することが必要となる。図６１の処理から説明する。

【０３１１】まず、ユーザ機器とログ収集サーバは、相互認証を実行（Ｓ１５２１，Ｓ１７２１）しセッション鍵の生成を行なう。ユーザ機器は認証成立を条件として、ユーザ機器デバイス内のメモリに格納された購入ログを取り出して、購入ログに対してセッション鍵Ｋｓｅｓで改竄チェック値（ＩＣＶ１）を生成して購入ログ＋ＩＣＶ１をログ収集サーバに送信（Ｓ１５２２）する。

【０３１２】ログ収集サーバは、購入ログ＋ＩＣＶ１を受信（Ｓ１７２２）し、ＩＣＶ１の検証を実行（Ｓ１７２３）し、検証ＯＫの場合は、ログをデータベース内に保存（Ｓ１７２４）する。なお、ログ収集サーバは、さらに、購入ログ中のユーザ機器の電子署名の検証処理を行なって、データ改竄の有無を更にチェックする構成としてもよい。ログ収集サーバは、さらに、ログ受信ＯＫデータにセッション鍵Ｋｓｅｓで改竄チェック値（ＩＣＶ２）を生成し、ログ受信ＯＫデータ＋ＩＣＶ２をユーザ機器に送信（Ｓ１７２５）する。ステップＳ１７２３のＩＣＶ１の検証ＮＧであったときは、ログ受信ＮＧデータにセッション鍵Ｋｓｅｓで改竄チェック値（ＩＣＶ２）を生成し、ログ受信ＮＧデータ＋ＩＣＶ２をユーザ機器に送信（Ｓ１７２６）する。

【０３１３】ユーザ機器は、ログ受信データ＋ＩＣＶ２を受信（Ｓ１５２３）し、ＩＣＶ２の検証ＯＫ、ログ受信ＯＫ（Ｓ１５２４）である場合は、更新用の公開鍵（ＫｐＤＥＶ）と秘密鍵（ＫｓＤＥＶ）のペアを生成（Ｓ１５２５）し、生成した公開鍵（ＫｐＤＥＶ）に改竄チェック値（ＩＣＶ３）を生成付加してログ収集サーバに送信（Ｓ１５２６）する。

【０３１４】ログ収集サーバは、公開鍵（ＫｐＤＥＶ）＋ＩＣＶ３をユーザ機器から受信する（Ｓ１７２７）と、ＩＣＶ３の検証を実行（Ｓ１７３１）し、検証ＯＫである場合は公開鍵受信ＯＫメッセージに対するＩＣＶ４を生成付加してユーザ機器に送信（Ｓ１７３２）する。ＩＣＶ３の検証がＮＧである場合は公開鍵受信ＮＧメッセージにＩＣＶ４を生成付加してユーザ機器に送信（Ｓ１７３３）する。

【０３１５】さらに、ログ収集サーバは、公開鍵受信ＯＫメッセージに対するＩＣＶ４を生成付加してユーザ機器に送信（Ｓ１７３２）した場合、発行局（ＣＡ）に対して受領公開鍵とともに、公開鍵証明書の発行を要求して、ユーザ機器の更新された公開鍵証明書（Ｃｅｒｔ＿ＤＥＶ）を取得（Ｓ１７３４）し、さらに、更新された公開鍵証明書（Ｃｅｒｔ＿ＤＥＶ）に対する改竄チェック値ＩＣＶ５を生成付加してユーザ機器に送信（Ｓ１７３５）する。

【０３１６】ユーザ機器は、公開鍵受信結果（ＯＫまたはＮＧ）＋ＩＣＶ４を受信した後、ＩＣＶ４の検証を行ない、ＩＣＶ４検証ＯＫであり、公開鍵受信ＯＫ（Ｓ１５３２）である場合には、更新された公開鍵証明書＋ＩＣＶ５の受信（Ｓ１５３３）を実行し、ＩＣＶ５の検証、受信した公開鍵証明書の検証（Ｓ１５３４）を実行する。いずれの検証もＯＫである場合は、公開鍵証明書内の公開鍵を取り出して、自己の送信した公開鍵との比較（Ｓ１５３５）を行ない、一致した場合は更新用に生成した秘密鍵、および受領した公開鍵証明書をユーザ機器内のメモリに保存（Ｓ１５３６）し、ログ（ログ収集サーバに送付済みのログ）の消去処理（Ｓ１５３７）を実行する。

【０３１７】ステップＳ１５３２、Ｓ１５３４、Ｓ１５３５のいずれかの判定がＮｏである場合は、有効な公開鍵証明書の更新処理は実行されず、処理は終了する。

【０３１８】次に、コンテンツプロバイダとログ収集サーバ間で実行されるコンテンツ売り上げ確認処理について図６３のフローに基づいて説明する。ログ収集サーバは、ユーザ機器から受領する購入ログに基づいてコンテンツ料金の１または複数の料金受領エンティテイに対する料金配分情報を管理し、料金受領エンティテイからの売り上げ確認要求に応じて料金配分情報に基づく応答処理を実行する。ログ収集サーバは、購入ログに含まれるコンテンツＩＤと予めログ収集サーバが保有するコンテンツ料金配分情報から、コンテンツの売り上げに基づく料金受領エンティテイの売り上げを算出することができる。なお、図５５（Ｂ）に示す販売確認データを格納したログを受領する構成である場合は、販売確認データに含まれる分配情報に基づいて料金受領エンティテイの売り上げを算出することができる。

【０３１９】まず、コンテンツプロバイダとログ収集サーバ間において、相互認証（Ｓ１５２１，Ｓ１７２１）が実行され、セッション鍵Ｋｓｅｓが生成される。ログ収集サーバは、相互認証の成立を条件として、コンテンツプロバイダ（ＣＰ）の公開鍵証明書Ｃｅｒｔ＿ＣＰからコンテンツプロバイダの識別子ＩＤ＿ＣＰを取り出し（Ｓ１７２２）、ＩＤ＿ＣＰに対応する売り上げデータをデータベースに格納したログ情報に基づいて生成（Ｓ１７２３）する。収集したログデータには、前述したようにコンテンツプロバイダの配分情報が格納されており、ログデータに基づいて各コンテンツプロバイダの配分料金が求められる。さらに、ログ収集サーバは、売り上げデータに対する改竄チェック値ＩＣＶ１を生成付加してコンテンツプロバイダ（ＣＰ）に送信（Ｓ１７２４）する。

【０３２０】コンテンツプロバイタ（ＣＰ）は、ログ収集サーバから売り上げデータ＋ＩＣＶ１を受信（Ｓ１５２２）し、ＩＣＶ１の検証を行なってデータ改竄のないことを確認して（Ｓ１５２３）売り上げデータをメモリに保存（Ｓ１５２４）する。ＩＣＶ１の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ログ収集サーバに対する売り上げデータ要求を行なう。

【０３２１】次に、ショップサーバとログ収集サーバ、コンテンツプロバイダ間で実行される売り上げ報告処理について図６４、図６５の処理フローに基づいて説明する。ショップサーバは、コンテンツの売り上げデータを管理し、ログ収集サーバに対して、所定期間内の全売り上げてデータまたは、料金受領エンティテイ毎の売り上げデータを送信する処理を実行する。図６４は、ショップサーバが実行したコンテンツ販売処理全体の売り上げを一括してログ収集サーバに送信する処理であり、図６５の処理は、ショップサーバが実行したコンテンツ販売処理中、特定のコンテンツプロバイダの提供したコンテンツに関する売り上げを選択してコンテンツプロバイダに送信する処理である。

【０３２２】図６４の売り上げ一括報告処理から説明する。まず、ショップサーバとログ収集サーバ間において、相互認証（Ｓ１６３１，Ｓ１７３１）が実行され、セッション鍵Ｋｓｅｓが生成される。ショップサーバは、相互認証の成立を条件として、所定期間の全売り上げデータをデータベースから取り出し、全売り上げデータに対する改竄チェック値ＩＣＶ１を生成付加してログ収集サーバに送信（Ｓ１６３２）する。

【０３２３】ログ収集サーバは、ショップサーバから全売り上げデータ＋ＩＣＶ１を受信（Ｓ１７３２）し、ＩＣＶ１の検証を行なってデータ改竄のないことを確認して（Ｓ１７３３）、売り上げデータをメモリに保存（Ｓ１７３４）する。ＩＣＶ１の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ショップサーバに対する売り上げデータ要求を行なう。

【０３２４】図６５の特定コンテンツプロバイダ売り上げ報告処理について説明する。まず、ショップサーバとコンテンツプロバイダ間において、相互認証（Ｓ１６４１，Ｓ１７４１）が実行され、セッション鍵Ｋｓｅｓが生成される。ショップサーバは、相互認証の成立を条件として、相互認証で得られたコンテンツプロバイダの公開鍵証明書Ｃｅｒｔ＿ＣＰからコンテンツプロバイダの識別子であるＩＤ＿ＣＰを取り出し（Ｓ１６４２）、取り出したＩＤ＿ＣＰに基づいて、売り上げデータの検索を行ない、その特定コンテンツプロバイダの提供コンテンツの売り上げデータを取得（Ｓ１６４３）する。さらに売り上げデータに対する改竄チェック値ＩＣＶ１を生成付加してログ収集サーバに送信（Ｓ１６４４）する。

【０３２５】ログ収集サーバは、ショップサーバから全売り上げデータ＋ＩＣＶ１を受信（Ｓ１７４２）し、ＩＣＶ１の検証を行なってデータ改竄のないことを確認して（Ｓ１７４３）、売り上げデータをメモリに保存（Ｓ１７４４）する。ＩＣＶ１の検証を行なってデータ改竄ありの場合は、メモリに対するデータ保存を実行せず、処理を終了する。この場合は、再度、ショップサーバに対する売り上げデータ要求を行なう。

【０３２６】本実施例の構成によれば、ユーザ機器の公開鍵証明書の更新処理に応じてコンテンツ購入ログデータを収集することが可能となり、ログ収集サーバを管理するシステム運営者（ＳＨ：System Holder）は、コンテンツ売り上げ状況を確実に把握することが可能となる。ユーザ機器の公開鍵証明書は、ショップサーバとの相互認証処理において必要であり、有効な期限の設定された公開鍵証明書を有することがコンテンツ購入を実行するための条件となる。また、ユーザ機器からの購入要求データ等に付加される署名の検証もユーザ機器の公開鍵証明書から取り出される公開鍵によって実行されることになり、有効な期限の設定された公開鍵証明書を有することが署名検証においても必要となる。従って、ユーザ機器は、コンテンツ購入を行なうためには、ログデータをログ収集サーバに送信し、公開鍵証明書の更新を行ない有効な期限を持つ公開鍵証明書を有することが必要となる。公開鍵証明書の有効期限を例えば１ヶ月、または３ヶ月等に設定することにより、ログ収集サーバを管理するシステム運営者（ＳＨ：System Holder）は、各設定機関毎の蓄積ログを確実に収集することができる。

【０３２７】上述したように、システム運営者の管理するログ収集サーバにより確実にユーザ機器からのログデータが収集され、コンテンツ売り上げ状況を管理することが可能となる。さらに、ログデータ中の売り上げ配分情報に基づいて、コンテンツ売り上げをコンテンツプロバイダ等の売り上げ利益取得権利者に対して正確な配分が可能となる。

【０３２８】また、本実施例では、各エンティテイ間において通信されるデータに相互認証時に生成したセッション鍵Ｋｓｅｓを改竄チェック値（ＩＣＶ）の生成鍵として用い、送信データにＩＣＶを付加して通信する構成としたので、通信データの安全性がさらに高まることになる。

【０３２９】なお、上述した実施例では、ユーザ機器とショップサーバ間の相互認証処理、署名生成、署名検証処理のいずれも実行する構成として説明したが、いずれかのみの処理、すなわち、相互認証のみ、あるいは署名生成、署名検証処理のみを実行する構成として、いずれかにおいて有効期限内の公開鍵証明書の利用を必須とする構成としてもよい。

【０３３０】［４．属性データを記録した公開鍵証明書または属性証明書利用構成］次に、属性データを記録し

た公開鍵証明書または属性証明書の利用構成について説明する。例えば上述したコンテンツ配信構成において、悪意のショップ運営者がユーザ機器になりすましてコンテンツの架空取り引きを実行したり、あるいはコンテンツプロバイダとショップ間における架空コンテンツ取り引きを行なう可能性がある。また、正当な取り引きを実行しようとするユーザ機器がショップサーバであると信じて通信を開始し、ショップサーバ相手のコンテンツ購入要求を実行して、例えばクレジット口座番号の送信処理を実行するような場合、相手がショップサーバになりすました不正なサーバであるような場合は、ユーザ機器からクレジット口座番号を不正に取得する等の処理が実行されるおそれがある。さらに、ユーザ機器がショップになりすまして、他のユーザ機器に対してコンテンツの架空販売を行なうなどの処理を行なう可能性も否定できない。このような事態が発生すると、システム運営者は正確なコンテンツ配信実体を把握することが困難となる。

【０３３１】このような正規なコンテンツ配信ルート以外の架空取引等を防止する構成として、以下、属性データを記録した公開鍵証明書または属性証明書利用構成を説明する。

【０３３２】属性データとは、ユーザ機器（ＤＥＶＩＣＥ）、ショップ（ＳＨＯＰ）、コンテンツプロバイダ（ＣＰ）、サービス運営者（ＳＨ）、公開鍵証明書、属性証明書の発行審査を行なう登録局等、コンテンツ配信システムを構成するエンティテイの種別を識別するデータである。

【０３３３】属性データの構成例として、属性データの内容を示すテーブルを図６６に示す。図６６に示すように、異なるコードが各エンティテイに割り当てられる。例えば、ユーザ機器あるいはショップ等から公開鍵証明書、属性証明書の発行要求を受けつけ、審査を行なう登録局には「０００００」、コンテンツ配信システム上で流通するコンテンツに対するライセンスを徴収するシステムホルダとしてのサービス運営者には「００００１」が属性コードとして割り振られる。上述した例では、サービス運営者は鍵かけかえ処理を実行するユーザ機器認証サーバを管理するエンティテイであったり、また、ログ情報を収集するログ情報収集サーバを管理するエンティテイである。

【０３３４】さらに、ユーザ機器に対してコンテンツを販売するショップとしてのコンテンツ販売者には、「００００２」、ショップ（コンテンツ販売者）からの要求に応じてコンテンツをユーザに配信する配信サーバの運営エンティテイであるコンテンツ配信者には、「００００３」、コンテンツを購入し利用するユーザ機器には「００００４」のコードが割り当てられる。この他にもコンテンツ配信に係わるエンティテイに対して、その種類に応じて異なるコードが割り当てられる。なお、ショップに必ずしも１つのコードを割り当てる構成に限らず、役割、機能の異なるショップがある場合には、異なるコードを割り当てて、それぞれを区別可能にしてもよいし、またユーザ機器にも、何らかのカテゴリに応じて異なる属性コードを割り当てる構成としてもよい。

【０３３５】上述した属性情報は、公開鍵証明書に含める構成と、公開鍵証明書とは異なる属性証明書を発行し、属性証明書によって属性を識別する構成とがある。属性情報を持つ公開鍵証明書の構成例を図６７に示す。

【０３３６】図６７に示す公開鍵証明書は、証明書のバージョン番号、公開鍵証明書発行局（ＣＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前（ｅｘ．ユーザ機器ＩＤ）、証明書利用者の公開鍵、さらに、上述した［００００］，［０００１］…［ｎｎｎｎ］等の属性情報、さらに電子署名を含む。証明書の通し番号は、例えば発行年（４バイト）、月（２バイト）、日（２バイト）、シリアル番号（８バイト）の合計１６バイトとする。利用者名は、登録局の定める識別可能な名前、あるいは乱数、通し番号を用いてもよい。あるいは上位バイトをカテゴリとし、下位バイトを通し番号とする構成としてもよい。

【０３３７】電子署名は、証明書のバージョン番号、公開鍵証明書発行局（ＣＡ）が証明書利用者に対し割り付ける証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前、証明書利用者の公開鍵、並びに属性データ全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して発行局の秘密鍵を用いて生成したデータである。

【０３３８】公開鍵証明書発行局（ＣＡ）は、図６７に示す公開鍵証明書を発行するとともに、有効期限が切れた公開鍵証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。

【０３３９】一方、この公開鍵証明書を利用する際には、利用者は自己が保持する発行局の公開鍵ＫｐＣＡを用い、当該公開鍵証明書の電子署名を検証し、電子署名の検証に成功した後に公開鍵証明書から公開鍵を取り出し、当該公開鍵を利用する。従って、公開鍵証明書を利用する全ての利用者は、共通の公開鍵証明書発行局の公開鍵を保持している必要がある。

【０３４０】次に図６８に属性情報を持たない公開鍵証明書と、属性証明書のデータ構成を示す。（Ａ）は属性情報を持たない公開鍵証明書であり、図６７に示す公開鍵証明書から属性情報を取り除いたデータ構成であり、公開鍵証明書発行局が発行する。（Ｂ）は属性証明書である。属性証明書は、属性証明書発行局（ＡＡ：Attribute Authority）が発行する。

【０３４１】図６８に示す属性証明書は、証明書のバージョン番号、属性証明書発行局（ＡＡ）が発行する属性証明書に対応する公開鍵証明書の通し番号、これは対応公開鍵証明書の証明書の通し番号と同一であり、両証明書を関連づけるリンクデータとしての機能を持つ。属性証明書によって通信相手の属性を確認しようとするエンティテイは、公開鍵証明書とリンクする属性証明書を、公開鍵証明書および属性証明書に共通に格納された公開鍵証明書通し番号に基づいて確認し、公開鍵証明書と同一の公開鍵証明書通し番号を格納した属性証明書から属性情報を取得することができる。通し番号は、例えば発行年（４バイト）、月（２バイト）、日（２バイト）、シリアル番号（８バイト）の合計１６バイトとする。さらに、電子署名に用いたアルゴリズムおよびパラメータ、属性証明書発行局の名前、証明書の有効期限、証明書利用者の名前（ｅｘ．ユーザ機器ＩＤ）、これは、対応する公開鍵証明書の利用者名と同一であり、登録局の定める識別可能な名前、あるいは乱数、通し番号、あるいは上位バイトをカテゴリとし、下位バイトを通し番号としたデータ構成である。さらに、上述した［００００］，［０００１］…［ｎｎｎｎ］等の属性情報、属性証明書発行局（ＡＡ）の電子署名を含む。

【０３４２】電子署名は、証明書のバージョン番号、公開鍵証明書の通し番号、電子署名に用いたアルゴリズムおよびパラメータ、発行局の名前、証明書の有効期限、証明書利用者の名前、並びに属性データ全体に対しハッシュ関数を適用してハッシュ値を生成し、そのハッシュ値に対して属性証明書発行局の秘密鍵を用いて生成したデータである。

【０３４３】属性証明書発行局（ＡＡ）は、図６８（Ｂ）に示す属性証明書を発行するとともに、有効期限が切れた属性証明書を更新し、不正を行った利用者の排斥を行うための不正者リストの作成、管理、配布（これをリボケーション：Revocationと呼ぶ）を行う。

【０３４４】図６９にコンテンツ取り引きに参加するユーザ機器、ショップサーバがそれぞれ使用する公開鍵証明書を新規に発行する手続きを説明する図を示す。なお、ここでショップサーバ１０１０、ユーザ機器１０２０は、前述の図１他で説明したと同様の構成を持つ。サービス運営体１０３０は、コンテンツ配信全体を管理するシステムホルダ（ＳＨ）であり、前述したコンテンツ鍵のかけかえ処理、あるいはユーザ機器のコンテンツ購入により生成されるログを収集する等の手法により、コンテンツの流通状況を把握する。ここでは、さらに、ショップサーバ１０１０、ユーザ機器１０２０他の公開鍵証明書および属性証明書の発行要求の受付、審査を実行する登録局（ＲＡ：Registration Authority）としての機能も兼ね備える。なお、本例ではサービス運営体１０３０がシステムホルダ（ＳＨ）としての機能と、登録局（ＲＡ）としての機能を持つ構成であるが、これらは別々の独立したエンティテイとして構成してもよい。

【０３４５】図６９では、ユーザ機器１０２０における公開鍵証明書の新規発行手続きをＡ１～Ａ８で示し、ショップサーバ１０１０の公開鍵証明書の新規発行手続きをＢ１～Ｂ７で示している。まず、ユーザ機器１０２０における公開鍵証明書の新規発行手続きについて説明する。

【０３４６】（Ａ１）相互認証

まず、ユーザ機器１０２０は、サービス運営体１０３０との間で相互認証を実行する。ただし、この時点でユーザ機器１０２０は、公開鍵証明書を保有していないので、公開鍵証明書を用いた相互認証を実行することはできず、先に図１２を用いて説明した対称鍵暗号方式、すなわち、共有秘密鍵、識別子（ＩＤ）を用いた相互認証処理を実行（詳細は図１２に関する説明を参照）する。

【０３４７】（Ａ２）公開鍵、秘密鍵ペア生成

（Ａ３）公開鍵証明書発行要求

（Ａ４）審査＆公開鍵証明書発行要求

（Ａ５）公開鍵証明書発行要求

相互認証が成立すると、ユーザ機器１０２０は、自己のデバイス内の暗号処理部において、新規に登録する公開鍵と秘密鍵のペアを生成し、生成した公開鍵をサービス運営体１０３０に対して、証明書発行要求とともに送信する。公開鍵証明書発行要求を受信したサービス運営体１０３０は、発行要求を審査し、公開鍵証明書を発行するエンティテイとしての要件を満足している場合に、証明書発行要求を公開鍵証明書発行局（ＣＡ）１０４０に対して送信する。なお、ここで発行する公開鍵証明書が図６８（Ａ）に示す属性情報を持つ公開鍵証明書である場合は、サービス運営体１０３０は、証明書発行要求を送信してきたエンティテイの属性をＩＤに基づいて判定する。

【０３４８】コンテンツ配信に参加するユーザ機器には、予めユーザ機器識別子（ＩＤ）および秘密情報としての秘密鍵が格納され、これらユーザ機器ＩＤ、秘密鍵はサービス運営体１０３０によって管理された構成であり、サービス運営体１０３０は、ユーザ機器から送信されるＩＤに基づき秘密情報格納データベースを検索し、予め登録済みのユーザ機器ＩＤであることを確認した後、秘密鍵を取り出し、この鍵を用いてユーザ機器と図１２に基づく相互認証を行ない、相互認証に成功した場合にのみコンテンツ配信に参加可能なユーザ機器であることを確認する。

【０３４９】（Ａ６）公開鍵証明書発行

（Ａ７）公開鍵証明書送信

（Ａ８）公開鍵証明書送信

サービス運営体１０３０からの公開鍵証明書発行要求を受信した公開鍵証明書発行局１０４０は、ユーザ機器の公開鍵を格納し、公開鍵証明書発行局１０４０の電子署名を持つ公開鍵証明書（図６７または図６８（Ａ））を

発行し、サービス運営体１０３０に送信する。サービス運営体１０３０は、公開鍵証明書発行局１０４０から受信した公開鍵証明書をユーザ機器１０２０に対して送信する。ユーザ機器は、受信した公開鍵証明書と先ほど（Ａ２）で生成しておいた秘密鍵を自デバイス内に格納し、コンテンツ取り引きの際の相互認証、データ暗号化、復号処理等に使用可能となる。

【０３５０】一方、ショップサーバ１０１０の公開鍵証明書の発行手続きは、基本的にユーザ機器における証明書発行手続きと同様であるが、ショップサーバは、コンテンツの販売を手がけるエンティテイとしてサービス運営体１０３０に認可してもらう手続きが必要となる。従って、ショップサーバ１０１０は、自己の公開鍵とともに、ライセンス申請（図６９、Ｂ２の手続き）を実行することが必要となる。これは、例えばサービス運営体１０３０が定めるポリシーに従ったコンテンツ販売を実行することをショップサーバ１０１０が受諾する処理として実行されるものである。サービス運営体１０３０は、ショップサーバ１０１０がサービス運営体１０３０が定めるポリシーに従ったコンテンツ販売を実行可能であり、ショップサーバ１０１０がポリシーを遵守することを受諾した場合には、ショップに対する公開鍵証明書の発行手続きを進める。公開鍵証明書の発行手続き処理は、上述したユーザ機器の場合と同様である。

【０３５１】次に、公開鍵証明書の更新処理について図７０を用いて説明する。公開鍵証明書は図６７，図６８（Ａ）に示すように有効期限が定められており、公開鍵証明書を使用するエンティテイは有効期限のすぎた証明書は使用できないので、有効期限内に更新処理を実行し、新たな有効期限の設定された公開鍵証明書の発行手続きを行なうことが必要となる。

【０３５２】図７０において、ユーザ機器１０２０における公開鍵証明書の更新手続きをＡ１～Ａ８で示し、ショップサーバ１０１０の公開鍵証明書の更新手続きをＢ１～Ｂ７で示している。まず、ユーザ機器１０２０における公開鍵証明書の更新手続きについて説明する。

【０３５３】（Ａ１）相互認証

まず、ユーザ機器１０２０は、サービス運営体１０３０との間で相互認証を実行する。この時点でユーザ機器１０２０は、現在有効な公開鍵証明書を保有しているので、公開鍵証明書を用いた相互認証を実行する。これは先に図１３を用いて説明した相互認証処理である。なお、すでに手持ちの公開鍵証明書の有効期限がすぎている場合は、新規発行手続きと同様先に図１２を用いて説明した共有秘密鍵、識別子（ＩＤ）を用いた相互認証処理を実行するようにしてもよい。

【０３５４】（Ａ２）新規公開鍵、秘密鍵ペア生成

（Ａ３）公開鍵証明書更新要求

（Ａ４）審査＆公開鍵証明書更新要求

（Ａ５）公開鍵証明書更新要求

相互認証が成立すると、ユーザ機器１０２０は、自己のデバイス内の暗号処理部において、更新用の新規公開鍵と秘密鍵のペアを生成し、生成した公開鍵をサービス運営体１０３０に対して、証明書更新要求とともに送信する。公開鍵証明書更新要求を受信したサービス運営体１０３０は、更新要求を審査し、更新要件を満足している場合に、証明書更新要求を公開鍵証明書発行局（ＣＡ）１０４０に対して送信する。なお、ここで発行する公開鍵証明書が図６８（Ａ）に示す属性情報を持つ公開鍵証明書である場合は、サービス運営体１０３０は、証明書発行要求を送信してきたエンティテイの属性をＩＤに基づいて判定する。

【０３５５】（Ａ６）公開鍵証明書更新

（Ａ７）公開鍵証明書送信

（Ａ８）公開鍵証明書送信

サービス運営体１０３０からの公開鍵証明書更新要求を受信した公開鍵証明書発行局１０４０は、ユーザ機器の新規公開鍵を格納し、公開鍵証明書発行局１０４０の電子署名を持つ公開鍵証明書（図６７または図６８（Ａ））を発行し、サービス運営体１０３０に送信する。サービス運営体１０３０は、公開鍵証明書発行局１０４０から受信した公開鍵証明書をユーザ機器１０２０に対して送信する。ユーザ機器は、受信した公開鍵証明書と先ほど（Ａ２）で生成しておいた秘密鍵を自デバイス内に格納し、コンテンツ取り引きの際の相互認証、データ暗号化、復号処理等に使用可能となる。

【０３５６】一方、ショップサーバ１０１０の公開鍵証明書の更新手続きは、基本的にユーザ機器における証明書更新手続きと同様であるが、前述のライセンス申請の更新（図７０、Ｂ２の手続き）を実行することが必要となる。サービス運営体１０３０が、ショップサーバ１０１０のライセンス更新を認めた場合には、ショップに対する公開鍵証明書の更新手続きを進める。公開鍵証明書の更新手続き処理は、上述したユーザ機器の場合と同様である。

【０３５７】次に、図７１を用いて属性証明書の新規発行手続きについて説明する。属性証明書は、図６８（Ｂ）に示す証明書であり、図６８（Ａ）に示す公開鍵証明書の発行の後、属性証明書が発行される。図７１では、ユーザ機器１０２０における属性証明書の新規発行手続きをＡ１～Ａ７で示し、ショップサーバ１０１０の公開鍵証明書の新規発行手続きをＢ１～Ｂ７で示している。まず、ユーザ機器１０２０における公開鍵証明書の新規発行手続きについて説明する。

【０３５８】（Ａ１）相互認証

まず、ユーザ機器１０２０は、サービス運営体１０３０との間で相互認証を実行する。この時点でユーザ機器１０２０は、すでに公開鍵証明書発行局公開鍵証明書を保有しているので、公開鍵証明書を用いた相互認証を実行する。

【０３５９】（Ａ２）属性証明書発行要求
（Ａ３）審査＆属性証明書発行要求
（Ａ４）属性証明書発行要求
相互認証が成立すると、ユーザ機器１０２０は、サービス運営体１０３０に対して、属性証明書発行要求を送信する。属性証明書発行要求を受信したサービス運営体１０３０は、発行要求を審査し、属性証明書を発行するエンティテイとしての要件を満足している場合に、証明書発行要求を属性証明書発行局（ＡＡ）１０５０に対して送信する。なお、ここでサービス運営体１０３０は、証明書発行要求を送信してきたエンティテイの属性をＩＤに基づいて判定する。前述したように、コンテンツ配信に参画するユーザ機器には、予めユーザ機器識別子（ＩＤ）が格納され、これらユーザ機器ＩＤはサービス運営体１０３０によって管理された構成であり、サービス運営体１０３０は、ユーザ機器から送信されるＩＤと、予め登録済みのユーザ機器ＩＤと比較参照することにより、コンテンツ配信に参画可能なユーザ機器であることを確認する。
【０３６０】（Ａ５）属性証明書発行
（Ａ６）属性証明書送信
（Ａ７）属性証明書送信
サービス運営体１０３０からの属性証明書発行要求を受信した属性証明書発行局１０５０は、ユーザ機器の属性情報を格納し、属性証明書発行局１０５０の電子署名を持つ属性証明書（図６８（Ｂ））を発行し、サービス運営体１０３０に送信する。サービス運営体１０３０は、属性証明書発行局１０５０から受信した属性証明書をユーザ機器１０２０に対して送信する。ユーザ機器は、受信した属性証明書を自デバイス内に格納し、コンテンツ取り引きの際の属性確認処理に使用する。
【０３６１】一方、ショップサーバ１０１０の属性証明書の発行手続き（Ｂ１～Ｂ７）は、基本的にユーザ機器における証明書発行手続きと同様である。また、属性証明書の更新手続きも新規発行手続きと同様の手続きとなる。
【０３６２】次に、属性証明書による属性確認処理、または公開鍵証明書に格納された属性情報による属性確認処理を伴うコンテンツ取り引きについて説明する。
【０３６３】図７２に相互認証時に併せて属性確認処理を実行する処理構成を示す。図７２の構成は、先に説明した図１のシステム構成と同様である。すなわち、コンテンツの販売を実行するショップサーバ１０１０、コンテンツ購入を実行するユーザ機器１０２０、ユーザ機器認証サーバ１０３０を構成要素とする。ここで、ユーザ機器認証サーバ１０３０は、前述したサービス運営体の管理下にある。図７２の番号（１）から（２０）の順に処理が進行する。各番号順に処理の詳細を説明する。
【０３６４】（１）相互認証および属性確認処理
コンテンツをショップサーバ１０１０から購入しようとするユーザ機器１０２０は、ショップサーバとの間で相互認証処理を行なう。データ送受信を実行する２つの手段間では、相互に相手が正しいデータ通信者であるか否かを確認して、その後に必要なデータ転送を行なうことが行われる。相手が正しいデータ通信者であるか否かの確認処理が相互認証処理である。相互認証処理時にセッション鍵の生成を実行して、生成したセッション鍵を共有鍵として暗号化処理を実行してデータ送信を行なう構成が１つの好ましいデータ転送方式である。公開鍵方式の相互認証処理は、公開鍵証明書の発行局の署名検証の後、相手型の公開鍵を取り出して実行される。詳細は前述の図１３に関する説明を参照されたい。
【０３６５】さらに、本実施例においては、属性確認処理を実行する。ショップサーバ１０１０は、通信相手の公開鍵証明書に属性データが格納されている場合は、その属性がユーザ機器であることを示すデータであることを確認する。公開鍵証明書に属性データが格納されていない場合は、属性証明書を用いて属性の確認を行なう。属性証明書には、属性証明書発行局の秘密鍵を用いて署名がなされているので、属性証明書発行局の公開鍵：ＫｐＡＡを用いて署名検証を実行し、正当な証明書であることを確認し、属性証明書の「通し番号」および／または「利用者（ＩＤ）」が、公開鍵証明書内の「通し番号」および／または「利用者（ＩＤ）」と一致しているか確認した後、証明書内の属性情報を確認する。
【０３６６】一方、ユーザ機器１０２０は、通信相手の公開鍵証明書に属性データが格納されている場合は、その属性がショップであることを示すデータであることを確認する。公開鍵証明書に属性データが格納されていない場合は、属性証明書について、属性証明書発行局の公開鍵：ＫｐＡＡを用いて署名検証を実行し、正当な証明書であることを確認し、属性証明書の「通し番号」および／または「利用者（ＩＤ）」が、公開鍵証明書内の「通し番号」および／または「利用者（ＩＤ）」と一致しているか確認した後、証明書内の属性情報を確認する。
【０３６７】ショップサーバ１０１０は、コンテンツ購入要求主体の公開鍵証明書または属性証明書の属性がユーザ機器であることを確認し、ユーザ機器１０２０は、コンテンツ購入要求先の公開鍵証明書または属性証明書の属性がショップであることを確認して、その後の処理に移行する。
【０３６８】属性確認処理のフローを図７３に示す。図７３（Ａ）は、公開鍵証明書に属性データが格納されている場合の公開鍵証明書を用いた属性確認処理であり、（Ｂ）は、属性証明書を用いた属性確認処理である。
【０３６９】図７３（Ａ）のフローから説明する。まず、ステップＳ２１０１において、公開鍵証明書を用いた相互認証処理を実行（図１３参照）し、認証が成立したことを条件として（Ｓ２１０２の判定Ｙｅｓ）、相手

ある。

【０３７６】暗号化コンテンツ鍵データ１（ショップ）は、先に説明した図１４（ｂ）に示す構成である。すなわち、コンテンツ購入の要求元であるユーザ機器１０２０の識別子であるユーザ機器ＩＤ、購入要求データ（図１４（ａ）のユーザ機器公開鍵証明書を除いたデータ）、コンテンツ取り引きに伴いショップサーバ１０１０が生成したショップ処理Ｎｏ．、暗号化コンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を有し、これらのデータに対するショップサーバ１０１０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ１（ショップ）には、ショップサーバ１０１０の公開鍵証明書が添付され、ユーザ機器１０２０に送付される。なお、ショップサーバ公開鍵証明書が既に前述の相互認証処理、あるいはその以前の処理において、ユーザ機器側に送付済みの場合は、必ずしも改めて送付する必要はない。

【０３７７】（６）受信データ検証

ショップサーバ１０１０から暗号化コンテンツ：Ｋｃ（content）と、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を受信したユーザ機器１０２０は、暗号化コンテンツ鍵データ１（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器１０２０は、まずショップサーバ１０１０から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｂ）に示す暗号化コンテンツ鍵データ１のショップ署名の検証を実行する。

【０３７８】（７）相互認証および属性確認処理

ユーザ機器１０２０が、ショップサーバ１０１０から暗号化コンテンツ：Ｋｃ（content）と暗号化コンテンツ鍵データ１（ショップ）を受信し、暗号化コンテンツ鍵データ１（ショップ）の検証を終えると、ユーザ機器１０２０は、ユーザ機器認証サーバ１０３０にアクセスし、ユーザ機器１０２０と、ユーザ機器認証サーバ１０３０間において相互認証処理および属性確認処理を実行する。この処理は、前述のショップサーバ１０１０とユーザ機器１０２０間の相互認証処理および属性確認処理と同様の手続きで実行される。

【０３７９】（８）暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求送信

ユーザ機器１０２０とユーザ機器認証サーバ１０３０との間の相互認証および属性確認が成立すると、ユーザ機器１０２０は、ユーザ機器認証サーバ１０３０に対して、先にショップサーバ１０１０から受信した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）と、暗号化コンテンツ鍵かけかえ要求を送信する。暗号化コンテンツ鍵データ（ユーザ機器）の構成は、先に説明した図１４（ｃ）に示す構成である。すなわち、暗号化コンテンツ鍵かけかえ要求の要求先であるユーザ機器認証サーバ１０３０の識別子であるユーザ機器認証サーバＩＤ、ショップサーバ１０１０から受領した暗号化コンテンツ鍵データ（図１４（ｂ）のショップ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するユーザ機器１０２０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ユーザ機器）には、ショップサーバ１０１０の公開鍵証明書と、ユーザ機器１０２０の公開鍵証明書が添付され、ユーザ機器認証サーバ１０３０に送付される。なお、ユーザ機器認証サーバ１０３０がユーザ機器公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０３８０】（９）受信データ検証

ユーザ機器１０２０から暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求（図１４（ｃ））を受信したユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器認証サーバ１０３０は、まずユーザ機器１０２０から受領したユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）の電子署名の検証を実行する。さらに、ショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバの公開鍵ＫｐＳＨＯＰを用いて図１４（ｃ）に示す暗号化コンテンツ鍵データ（ユーザ機器）に含まれる（５）暗号化コンテンツ鍵データ１のショップ署名の検証を実行する。また、ユーザ機器の送信した電文が図１４（ｃ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３８１】（１０）暗号化コンテンツ鍵かけかえ処理

ユーザ機器認証サーバ１０３０において、ユーザ機器１０２０から受信した暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求の検証が終了し、正当な鍵かけかえ要求であると判定すると、ユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵データ（ユーザ機器）に含まれる暗号化コンテンツ鍵、すなわち、コンテンツ鍵：Ｋｃをユーザ機器認証サーバ（ＤＡＳ）１０３０の公開鍵ＫｐＤＡＳで暗号化したデータ：ＫｐＤＡＳ（Ｋｃ）をユーザ機器認証サーバ１０３０の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、さらにコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで暗号化した暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する。すなわち、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。

【０３８２】この処理は先に図１６を用いて説明したように、暗号化コンテンツ鍵データ（ユーザ機器）から、ユーザ機器認証サーバ（ＤＡＳ）１０３０の公開鍵ＫｐＤＡＳで暗号化したコンテンツ鍵データ：ＫｐＤＡＳ（Ｋｃ）を取り出し、次に、ユーザ機器認証サーバ１０３０の秘密鍵ＫｓＤＡＳで復号してコンテンツ鍵Ｋｃを取得し、次に、復号により取得したコンテンツ鍵Ｋｃをユーザ機器の公開鍵：ＫｐＤＥＶで再暗号化して暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を生成する処理である。

【０３８３】（１１）相互認証および属性確認処理

ユーザ機器認証サーバ１０３０において、上述の暗号化コンテンツ鍵の鍵かけかえ処理が完了すると、ユーザ機器認証サーバ１０３０は、ショップサーバ１０１０にアクセスし、ユーザ機器認証サーバ１０３０とショップサーバ１０１０間において相互認証処理および属性確認処理を実行する。この処理は、前述のショップサーバ１０１０とユーザ機器１０２０間の相互認証処理および属性確認処理と同様の手続きで実行される。

【０３８４】（１２）暗号化コンテンツデータ送信

ユーザ機器認証サーバ１０３０とショップサーバ１０１０間の相互認証および属性確認処理が成立すると、ユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１０１０に送信する。暗号化コンテンツ鍵データ（ＤＡＳ）の構成は、先に説明した図１７（ｄ）に示す構成である。コンテンツ購入の要求先であるショップサーバ１０１０の識別子であるショップＩＤ、暗号化コンテンツ鍵データ（ユーザ機器）（図１４（ｃ）のショップおよびユーザ機器公開鍵証明書を除いたデータ）、さらに、前述の鍵かけかえ処理により、ユーザ機器認証サーバ１０３０が生成した暗号化コンテンツ鍵データ：ＫｐＤＥＶ（Ｋｃ）を有し、これらのデータに対するユーザ機器認証サーバ１０３０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ（ＤＡＳ）には、ユーザ機器認証サーバ１０３０と、ユーザ機器１０２０の公開鍵証明書が添付され、ショップサーバ１０１０に送付される。なお、ショップサーバが、これらの公開鍵証明書を既に保有済みである場合は、必ずしも改めて送付する必要はない。

【０３８５】また、ユーザ機器認証サーバ１０３０が信頼できる第三者機関であると認められる存在である場合は、暗号化コンテンツ鍵データ（ＤＡＳ）は、図１７（ｄ）に示すようにユーザ機器の生成した（8）暗号化コンテンツ鍵データ（ユーザ機器）をそのまま含むデータ構成とすることなく、図１８（ｄ’）に示すように、ユーザ機器ＩＤ、トランザクションＩＤ、コンテンツＩＤ、ショップ処理ＮＯ、ユーザデバイスの公開鍵で暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）の各データを、ユーザ機器認証サーバ１０３０が抽出して、これらに署名を付加して暗号化コンテンツ鍵データ（ＤＡＳ）としてもよい。この場合は、（8）暗号化コンテンツ鍵データ（ユーザ機器）の検証が不要となるので、添付する公開鍵証明書は、ユーザ機器認証サーバ１０３０の公開鍵証明書のみでよい。

【０３８６】（１３）受信データ検証

ユーザ機器認証サーバ１０３０から暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ））を受信したショップサーバ１０１０は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ショップサーバ１０１０は、まずユーザ機器認証サーバ１０３０から受領したユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ１０３０の公開鍵ＫｐＤＡＳを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行する。さらに、ユーザ機器の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器の公開鍵ＫｐＤＥＶを用いて図１７（ｄ）に示す暗号化コンテンツ鍵データ（ＤＡＳ）に含まれる（8）暗号化コンテンツ鍵データ（ユーザ機器）のユーザ機器署名の検証を実行する。また、ユーザ機器の送信した電文が図１４（ｃ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３８７】なお、先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１０１０が受領した場合は、ショップサーバ１０１０は、ユーザ機器認証サーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ１０３０の公開鍵ＫｐＤＡＳを用いて図１８（ｄ’）に示す暗号化コンテンツ鍵データ（ＤＡＳ）の電子署名の検証を実行するのみの処理となる。

【０３８８】（１４）相互認証および属性確認

（１５）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器１０２０は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。なお、この際、前の要求と異なるセッションで要求を実行する場合は、再度相互認証および属性確認を実行して、相互認証および属性確認が成立したことを条件として暗号化コンテンツ鍵要求データがユーザ機器１０２０からショップサーバ１０１０に送信される。また、ユーザ機器の送信した電文が図１４（ｃ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３８９】暗号化コンテンツ鍵要求データの構成は図１７（ｅ）に示す通りである。暗号化コンテンツ鍵要求データは、コンテンツ購入の要求先であるショップサーバ１０１０の識別子であるショップＩＤ、取り引きの識別子として、ユーザ機器１０２０の暗号処理手段が乱数

に基づいて生成するトランザクションＩＤ、さらに、ユーザ機器が購入を希望するコンテンツの識別子としてのコンテンツＩＤ、さらに、先にショップが生成し暗号化コンテンツ鍵データ１（ショップ）としてユーザ機器１０２０に送信してきたデータ（図１４（ｂ）参照）中に含まれるショップ処理Ｎｏ．を有し、これらのデータに対するユーザ機器の電子署名が付加されている。さらに、暗号化コンテンツ鍵要求データには、ユーザ機器の公開鍵証明書が添付され、ショップサーバ１０１０に送付される。なお、公開鍵証明書が既にショップ側に保管済みの場合は、必ずしも改めて送付する必要はない。

【０３９０】（１６）検証処理、および
（１７）課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１０１０は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、図１５を用いて説明したと同様の処理である。データ検証が済むと、ショップサーバ１０１０は、コンテンツの取り引きに関する課金処理を実行する。課金処理は、ユーザの取り引き口座からコンテンツ料金を受領する処理である。受領したコンテンツ料金は、コンテンツの著作権者、ショップ、ユーザ機器認証サーバ管理者など、様々な関係者に配分される。

【０３９１】この課金処理に至るまでには、ユーザ機器認証サーバ１０３０による暗号化コンテンツ鍵の鍵かけかえ処理プロセスが必須となっているので、ショップサーバ１０１０は、ユーザ機器間とのみの処理では課金処理が実行できない。また、ユーザ機器１０２０においても暗号化コンテンツ鍵の復号ができないので、コンテンツの利用ができない。ユーザ機器認証サーバは、図６を用いて説明したユーザ機器認証サーバ・ライセンス管理データベースに、すべての鍵かけかえ処理を実行したコンテンツ取り引き内容を記録しており、すべての課金対象となるコンテンツ取り引きが把握可能となる。従って、ショップ側単独でのコンテンツ取り引きは不可能となり、不正なコンテンツ販売が防止される。

【０３９２】（１８）暗号化コンテンツ鍵データ２（ショップ）送信

ショップサーバ１０１０における課金処理が終了すると、ショップサーバ１０１０は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器１０２０に送信する。

【０３９３】暗号化コンテンツ鍵データ２（ショップ）の構成は、先に説明した図１７（ｆ）に示す通りである。暗号化コンテンツ鍵要求の要求元であるユーザ機器１０２０の識別子であるユーザ機器ＩＤ、ユーザ機器認証サーバ１０３０から受領した暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ）のユーザ機器、ユーザ機器認証サーバ公開鍵証明書を除いたデータ）、を有し、これらのデータに対するショップサーバ１０１０の電子署名が付加されている。さらに、暗号化コンテンツ鍵データ２（ショップ）には、ショップサーバ１０１０の公開鍵証明書と、ユーザ機器認証サーバ１０３０の公開鍵証明書が添付され、ユーザ機器１０２０に送付される。なお、ユーザ機器１０２０がユーザ機器認証サーバ公開鍵証明書、ショップサーバ公開鍵証明書をすでに保有している場合は、必ずしも改めて送付する必要はない。

【０３９４】なお、ユーザ機器認証サーバ１０３０が信頼できる第三者機関であると認められる存在であり、ショップサーバ１０１０がユーザ機器認証サーバ１０３０から受信する暗号化コンテンツ鍵データ（ＤＡＳ）が先に説明した図１８（ｄ’）の簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）である場合は、ショップサーバ１０１０は、図１８（ｆ’）に示す暗号化コンテンツ鍵データ２（ショップ）をユーザ機器に送付する。すなわち、図１８（ｄ’）に示す簡略化した暗号化コンテンツ鍵データ（ＤＡＳ）にショップサーバの署名を付加したデータに、ショップサーバ１０１０の公開鍵証明書と、ユーザ機器認証サーバ１０３０の公開鍵証明書が添付してユーザ機器１０２０に送付する。

【０３９５】（１９）受信データ検証

ショップサーバ１０１０から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器１０２０は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図１５の処理フローと同様の処理であり、ユーザ機器１０２０は、まずショップサーバ１０１０から受領したショップサーバの公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したショップサーバ１０１０の公開鍵ＫｐＳＨＯＰを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）の電子署名の検証を実行する。さらに、ユーザ機器認証サーバ１０３０の公開鍵証明書の検証を発行局（ＣＡ）の公開鍵ＫｐＣＡを用いて実行し、次に公開鍵証明書から取り出したユーザ機器認証サーバ１０３０の公開鍵ＫｐＤＡＳを用いて図１７（ｆ）に示す暗号化コンテンツ鍵データ２（ショップ）に含まれる（１２）暗号化コンテンツ鍵データ（ＤＡＳ）の署名検証を実行する。また、何らかの送信電文が図１７（ｆ）に示すフォーマット中に入っている場合は、その電文の検証を必要に応じて実行する。

【０３９６】（２０）保存処理

ショップサーバ１０１０から受信した暗号化コンテンツ鍵データ２（ショップ）を検証したユーザ機器１０２０は、暗号化コンテンツ鍵データ２（ショップ）に含まれる自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器１０２０の記憶手段に格納する。コンテンツの利用時には、暗号化コンテン

ツ鍵：Ｋｓｔｏ（Ｋｃ）を保存鍵Ｋｓｔｏを用いて復号してコンテンツ鍵Ｋｃを取り出して、取り出したコンテンツ鍵Ｋｃを用いて、暗号化コンテンツＫｃ（Content）の復号処理を実行し、コンテンツ（Content）を再生、実行する。

【０３９７】以上、述べたように、コンテンツ配信に伴う各処理において、通信を実行する各エンティテイは、属性確認により、相手の属性、例えばユーザ機器であることを確認した後、処理を実行する構成としたので、不当なコンテンツ取り引き、例えばショップがユーザ機器になりすましてコンテンツを取り引きするなどの処理、あるいは、ショップサーバになりすまして、ユーザ機器からクレジット口座番号を不正に取得する等の処理が防止される。

【０３９８】例えばユーザ機器は、属性確認により、ユーザ機器の通信相手がショップであると確認されれば、ショップに対する処理としてのコンテンツ購入に伴う処理を安心して実行可能であり、また属性確認において、通信相手がユーザ機器認証サーバであると確認されれば、ユーザ機器認証サーバに対する処理、例えば鍵のかけかえ要求の送信を実行することができる。本構成によれば、属性確認を行なうことにより通信相手の属性が確認可能となるので、それぞれの通信相手に応じた正当な処理が実行される。さらに、不正な通信相手に秘密データを誤って送信することもなくなるので、データ漏洩の防止も可能である。

【０３９９】次に、相互認証処理による相手確認を実行せず、受信データの署名検証のみを実行して、データ改竄の有無と、属性確認を実行してコンテンツ取り引き処理を実行する形態について図７４を用いて説明する。

【０４００】図７４に示す処理は、図７２に示す処理から相互認証処理を省いた処理として実行されるものである。図７４の番号（１）から（１６）の順に処理が進行する。各番号順に処理の詳細を説明する。

【０４０１】（１）トランザクションＩＤ、購入要求データ生成、および

（２）購入要求データ送信

まず、ユーザ機器１０２０は、コンテンツの購入要求データを生成し、ショップサーバ１０１０に送信する。購入要求データの構成は、先に説明した図１４（ａ）に示す構成である。

【０４０２】（３）受信データ検証

図１４（ａ）に示す購入要求データをユーザ機器１０２０から受信したショップサーバは、受信データの検証処理を実行する。本実施例における検証処理は、購入要求データの改竄有無のチェックとともに、属性情報のチェックも併せて実行するものである。

【０４０３】図７５に公開鍵証明書に属性情報が格納されている場合の受信データ検証処理フローを示す。まず、メッセージと署名（購入要求データ）と、ユーザ機器の公開鍵証明書を受信（Ｓ２３０１）したショップサーバ１０１０は、ユーザ機器の公開鍵証明書を公開鍵証明書発行局の公開鍵ＫｐＣＡを用いて検証（Ｓ２３０２）する。検証が成立（Ｓ２３０３でＹｅｓ）すると、公開鍵証明書からユーザ機器の公開鍵：ＫｐＤＥＶを取り出し（Ｓ２３０４）て、ユーザ機器の公開鍵：ＫｐＤＥＶを用いて購入要求データのユーザ機器署名の検証（Ｓ２３０５）を行なう。さらに、検証が成功（Ｓ２３０６でＹｅｓ）すると、公開鍵証明書から属性情報を取り出し（Ｓ２３０７）て、正当な属性（ここではユーザ機器を示す属性）であるか否かを判定（Ｓ２３０８）し、正当である場合は、検証処理成功（Ｓ２３０９）として、次の処理に移行する。ステップＳ２３０３，Ｓ２３０６，Ｓ２３０８で判定がＮｏの場合は、検証処理失敗（Ｓ２３１０）として処理を中止する。

【０４０４】次に、公開鍵証明書と属性証明書を用いた受信データ検証処理について図７６のフローを用いて説明する。まず、メッセージと署名（購入要求データ）と、ユーザ機器の公開鍵証明書、属性証明書を受信（Ｓ２４０１）したショップサーバ１０１０は、ユーザ機器の公開鍵証明書を公開鍵証明書発行局の公開鍵ＫｐＣＡを用いて検証（Ｓ２４０２）する。検証が成立（Ｓ２４０３でＹｅｓ）すると、公開鍵証明書からユーザ機器の公開鍵：ＫｐＤＥＶを取り出し（Ｓ２４０４）て、ユーザ機器の公開鍵：ＫｐＤＥＶを用いて購入要求データのユーザ機器署名の検証（Ｓ２４０５）を行なう。さらに、検証が成功（Ｓ２４０６でＹｅｓ）すると、属性証明書を属性証明書発行局の公開鍵ＫｐＡＡを用いて検証（Ｓ２４０７）する。検証が成功（Ｓ２４０８でＹｅｓ）したことを条件として、属性証明書から属性情報を取り出し（Ｓ２４０９）て、正当な属性（ここではユーザ機器を示す属性）であるか否かを判定（Ｓ２４１０）し、正当である場合は、検証処理成功（Ｓ２４１１）として、次の処理に移行する。ステップＳ２４０３，Ｓ２４０６，Ｓ２４０８，Ｓ２４１０で判定がＮｏの場合は、検証処理失敗（Ｓ２４１２）として処理を中止する。

【０４０５】（４）暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショップ）送信

ショップサーバ１０１０において、購入要求データの検証が完了し、データ改竄のない正当なコンテンツ購入要求であると判定され属性が確認されると、ショップサーバ１０１０は、暗号化コンテンツおよび暗号化コンテンツ鍵データ１（ショップ）（図１４（ｂ）参照）をユーザ機器に送信する。

【０４０６】（５）受信データ検証

ショップサーバ１０１０から暗号化コンテンツ：Ｋｃ（content）と、図１４（ｂ）に示す暗号化コンテンツ鍵データ１（ショップ）を受信したユーザ機器１０２０は、暗号化コンテンツ鍵データ１（ショップ）の検証処

理および属性確認処理を実行する。この検証処理は、先に説明した図７５または図７６の処理フローと同様の処理である。この場合、公開鍵証明書または属性証明書の属性がショップを示していない場合は、処理が中止されることになる。

【０４０７】（６）暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求送信

次に、ユーザ機器１０２０は、ユーザ機器認証サーバ１０３０に対して、先にショップサーバ１０１０から受信した暗号化コンテンツ鍵ＫｐＤＡＳ（Ｋｃ）と、暗号化コンテンツ鍵かけかえ要求（図１４（ｃ）参照）を送信する。

【０４０８】（７）受信データ検証

ユーザ機器１０２０から暗号化コンテンツ鍵データ（ユーザ機器）および暗号化コンテンツ鍵かけかえ要求（図１４（ｃ））を受信したユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵かけかえ要求の検証処理を実行する。この検証処理は、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がユーザ機器でない場合は、処理が中止される。

【０４０９】（８）暗号化コンテンツ鍵かけかえ処理、

次に、ユーザ機器認証サーバ１０３０において、ＫｐＤＡＳ（Ｋｃ）→Ｋｃ→ＫｐＤＥＶ（Ｋｃ）の鍵かけかえ処理を実行する。

【０４１０】（９）暗号化コンテンツデータ送信

次に、ユーザ機器認証サーバ１０３０は、暗号化コンテンツ鍵データ（ＤＡＳ）をショップサーバ１０１０に送信する。暗号化コンテンツ鍵データ（ＤＡＳ）の構成は、先に説明した図１７（ｄ）に示す構成である。

【０４１１】（１０）受信データ検証

ユーザ機器認証サーバ１０３０から暗号化コンテンツ鍵データ（ＤＡＳ）（図１７（ｄ））を受信したショップサーバ１０１０は、暗号化コンテンツ鍵データ（ＤＡＳ）の検証処理を実行する。この検証処理は、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認が併せて実行される。この場合は公開鍵証明書または属性証明書の属性がユーザ機器認証サーバ（サービス運営体）でない場合は、処理が中止される。

【０４１２】（１１）暗号化コンテンツ鍵要求データ送信

次に、ユーザ機器１０２０は、暗号化コンテンツ鍵要求データをショップサーバに対して送信する。暗号化コンテンツ鍵要求データの構成は図１７（ｅ）に示す通りである。

【０４１３】（１２）検証処理、および

（１３）課金処理

暗号化コンテンツ鍵要求データをユーザ機器から受信したショップサーバ１０１０は、暗号化コンテンツ鍵要求データの検証処理を実行する。これは、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がユーザ機器でない場合は、処理が中止される。データ検証が済むと、ショップサーバ１０１０は、コンテンツの取り引きに関する課金処理を実行する。

【０４１４】（１４）暗号化コンテンツ鍵データ２（ショップ）送信

ショップサーバ１０１０における課金処理が終了すると、ショップサーバ１０１０は、暗号化コンテンツ鍵データ２（ショップ）をユーザ機器１０２０に送信する。暗号化コンテンツ鍵データ２（ショップ）の構成は、先に説明した図１７（ｆ）に示す通りである。

【０４１５】（１５）受信データ検証

（１６）保存処理

ショップサーバ１０１０から、暗号化コンテンツ鍵データ２（ショップ）を受領したユーザ機器１０２０は、暗号化コンテンツ鍵データ２（ショップ）の検証処理を実行する。この検証処理は、先に説明した図７５、図７６の処理フローと同様の処理であり、属性確認も併せて実行する処理である。この場合は公開鍵証明書または属性証明書の属性がショップでない場合は、処理が中止される。データ検証が済むと、ユーザ機器１０２０は、コンテンツの保存処理、すなわち自己の公開鍵ＫｐＤＥＶで暗号化された暗号化コンテンツ鍵：ＫｐＤＥＶ（Ｋｃ）を自己の秘密鍵ＫｓＤＥＶを用いて復号し、さらに、ユーザ機器の保存鍵Ｋｓｔｏを用いて暗号化して暗号化コンテンツ鍵：Ｋｓｔｏ（Ｋｃ）を生成して、これをユーザ機器１０２０の記憶手段に格納する処理を実行する。

【０４１６】このように、図７４に示す処理においては、相互認証時に属性確認を行なうのではなく、受信したデータの署名検証において、属性を確認する処理を実行する構成としたので、処理が簡略化され、コンテンツ取り引きに伴う処理の効率化が達成される。

【０４１７】なお、上述した属性データによる属性確認を適用した実施例では、サービス運営体において、鍵かけかえ処理を実行する構成について説明したが、例えば前述のログ収集サーバを適用した構成においても属性確認処理を適用することが可能である。その他一般的なデータ送受信を実行するエンティテイ間において、それぞれのエンティテイに特徴づけられた機能に基づいて属性を設定し、設定された属性を公開鍵証明書または属性証明書に格納し、これらの証明書を用いて通信相手の属性確認処理を実行することにより、さらにデータ通信の安全性、セキュリテイを高めることが可能となる。また、属性確認処理は、従来の相互認証処理、署名検証処理と併せて実行することが可能であるので、通常のデータ通信は、署名検証のみ、あるいは相互認証のみを行ない、必要に応じて属性確認処理を行なうなど、セキュリティ

度合いに応じて選択的に署名検証処理、相互認証処理、属性確認処理のいずれか、あるいは組み合わせて実行することが可能である。

【０４１８】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０４１９】

【発明の効果】上述したように、本発明のコンテンツ配信システムおよびコンテンツ配信方法によれば、コンテンツの購入要求を受け付けるショップサーバが、ユーザ機器のコンテンツ購入要求に対する課金処理が終了したことを条件として、ユーザ機器の格納鍵での復号可能な態様とした暗号化コンテンツ鍵をユーザ機器に送付する構成としたので、コンテンツの購入に伴う確実な課金処理が可能となる。

【０４２０】さらに、本発明のコンテンツ配信システムおよびコンテンツ配信方法によれば、ユーザ機器からのコンテンツ購入要求に基づいて、ユーザ機器認証サーバ（ＤＡＳ）の公開鍵で暗号化したコンテンツ鍵ＫｐＤＡＳ（Ｋｃ）をユーザ機器の公開鍵ＫｐＤＥＶで暗号化したコンテンツ鍵ＫｐＤＥＶ（Ｋｃ）にかけかえる処理をコンテンツ配信を管理するユーザ機器認証サーバが実行する構成としたので、ショップとユーザ機器間のコンテンツ取り引きをユーザ機器認証サーバが確実に把握することが可能となる。

【０４２１】さらに、本発明のコンテンツ配信システムおよびコンテンツ配信方法によれば、ユーザ機器、ショップ、ユーザ機器認証サーバ間で実行されるデータ通信では、相互認証処理あるいは署名生成、検証処理の少なくともいずれかを実行する構成としたので、データ通信のセキュリテイ、データ改竄のチェックが可能となる。

【図面の簡単な説明】

【図１】本発明のコンテンツ配信システムのシステム概要およびコンテンツ配信処理を説明する図である。

【図２】本発明のコンテンツ配信システムにおけるショップサーバの構成を示す図である。

【図３】本発明のコンテンツ配信システムにおけるショップサーバの購買管理データベースの構成を示す図である。

【図４】本発明のコンテンツ配信システムにおけるショップサーバの制御手段構成を示す図である。

【図５】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバの構成を示す図である。

【図６】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのライセンス管理データベースの構成を示す図である。

【図７】本発明のコンテンツ配信システムにおけるユーザ機器の構成を示す図である。

【図８】本発明のコンテンツ配信システムにおけるユーザ機器の購入管理データベース構成を示す図である。

【図９】本発明のコンテンツ配信システムにおける公開鍵証明書配布構成を示す図である。

【図１０】本発明のコンテンツ配信システムにおいて適用可能な署名生成処理を説明する図である。

【図１１】本発明のコンテンツ配信システムにおいて適用可能な署名検証処理を説明する図である。

【図１２】本発明のコンテンツ配信システムにおいて適用可能な相互認証（対称鍵方式）処理を説明する図である。

【図１３】本発明のコンテンツ配信システムにおいて適用可能な相互認証（非対称鍵方式）処理を説明する図である。

【図１４】本発明のコンテンツ配信システムにおいて各エンティテイ間で通信されるデータ構成を説明する図である。

【図１５】本発明のコンテンツ配信システムにおいて適用可能なデータ検証処理を説明する図である。

【図１６】本発明のコンテンツ配信システムにおいて実行される鍵かけかえ処理を説明する図である。

【図１７】本発明のコンテンツ配信システムにおいて各エンティテイ間で通信されるデータ構成を説明する図である。

【図１８】本発明のコンテンツ配信システムにおいて各エンティテイ間で通信されるデータ構成を説明する図である。

【図１９】本発明のコンテンツ配信システムにおいて実行されるコンテンツ鍵保存処理を説明する図である。

【図２０】本発明のコンテンツ配信システムにおけるショップサーバのステータス変遷を説明する図である。

【図２１】本発明のコンテンツ配信システムにおけるユーザ機器のステータス変遷を説明する図である。

【図２２】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのステータス変遷を説明する図である。

【図２３】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その１）を示す図である。

【図２４】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その２）を示す図である。

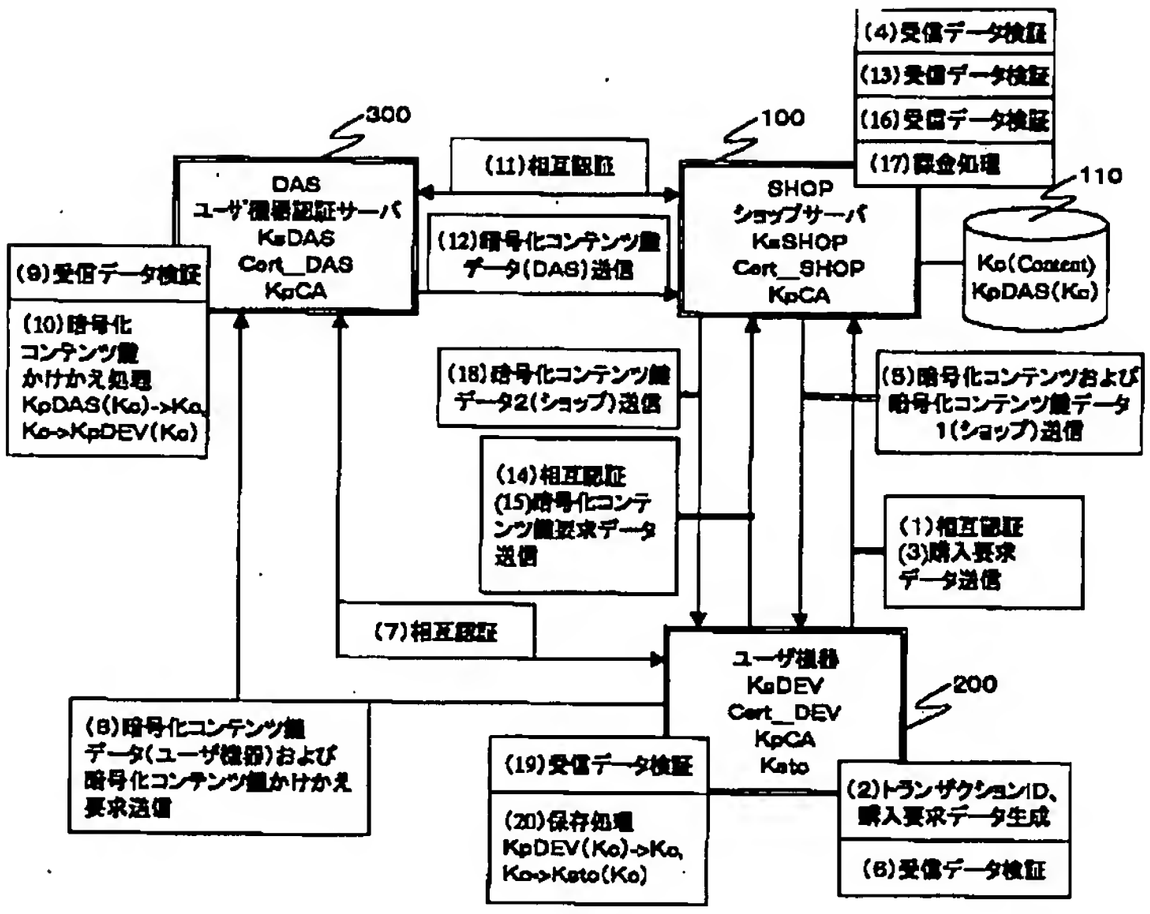
【図２５】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバとユーザ機器間の処理フローを示す図である。

【図２６】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバとショップサーバ間の処理フローを示す図である。

【図２７】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その１）を示す図である。
【図２８】本発明のコンテンツ配信システムにおけるショップサーバとユーザ機器間の処理フロー（その２）を示す図である。
【図２９】本発明のコンテンツ配信システムの変形例として配信サーバを用いたコンテンツ配信処理を説明する図である。
【図３０】本発明のコンテンツ配信システムの変形例として配信サーバを用いたコンテンツ配信処理を説明する図である。
【図３１】本発明のコンテンツ配信システムの変形例のコンテンツ配信処理を説明する図である。
【図３２】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図３３】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図３４】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図３５】本発明のコンテンツ配信システムの相互認証を伴わないコンテンツ配信処理を説明する図である。
【図３６】本発明のコンテンツ配信システムの相互認証を伴わないコンテンツ配信処理の変形例を説明する図である。
【図３７】本発明のコンテンツ配信システムにおいて電子チケットを適用したコンテンツ配信処理を説明する図である。
【図３８】本発明のコンテンツ配信システムのチケット発行サーバの構成を説明する図である。
【図３９】本発明のコンテンツ配信システムのチケット発行サーバのチケット発行管理データベース構成を説明する図である。
【図４０】本発明のコンテンツ配信システムのユーザ機器の購入管理データベース構成を説明する図である。
【図４１】本発明のコンテンツ配信システムのユーザ機器認証サーバのライセンス管理データベース構成を説明する図である。
【図４２】本発明のコンテンツ配信システムの配信サーバの構成を説明する図である。
【図４３】本発明のコンテンツ配信システムの配信サーバの配信管理データベース構成を説明する図である。
【図４４】本発明のコンテンツ配信システムのチケット換金サーバの構成を説明する図である。
【図４５】本発明のコンテンツ配信システムのチケット換金サーバのチケット換金管理データベース構成を説明する図である。
【図４６】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図４７】本発明のコンテンツ配信システムにおいて各エンティティ間で通信されるデータ構成を説明する図である。
【図４８】本発明のコンテンツ配信システムにおけるチケット発行サーバのステータス変遷を説明する図である。
【図４９】本発明のコンテンツ配信システムにおけるユーザ機器認証サーバのステータス変遷を説明する図である。
【図５０】本発明のコンテンツ配信システムにおける配信サーバのステータス変遷を説明する図である。
【図５１】本発明のコンテンツ配信システムにおけるユーザ機器のステータス変遷を説明する図である。
【図５２】本発明のコンテンツ配信システムにおけるチケット換金サーバのステータス変遷を説明する図である。
【図５３】本発明のコンテンツ配信システムにおいて電子チケットを適用したコンテンツ配信処理の具体例を説明する図である。
【図５４】本発明のコンテンツ配信システムにおいてログ収集サーバを適用したコンテンツ配信処理を説明する図である。
【図５５】本発明のコンテンツ配信システムにおける購入ログの構成例を説明する図である。
【図５６】本発明のコンテンツ配信システムにおけるログ収集サーバの構成を示す図である。
【図５７】本発明のコンテンツ配信システムにおけるユーザ機器と、ショップサーバ間の処理を示すフロー図（その１）である。
【図５８】本発明のコンテンツ配信システムにおけるユーザ機器と、ショップサーバ間の処理を示すフロー図（その２）である。
【図５９】本発明のコンテンツ配信システムにおける購入要求データと販売確認データのフォーマット例を示す図である。
【図６０】本発明のコンテンツ配信システムにおいて着ようか能な改竄チェック値（ＩＣＶ）生成処理構成を示す図である。
【図６１】本発明のコンテンツ配信システムにおけるユーザ機器と、ログ収集サーバ間の処理を示すフロー図（その１）である。
【図６２】本発明のコンテンツ配信システムにおけるユーザ機器と、ログ収集サーバ間の処理を示すフロー図（その２）である。
【図６３】本発明のコンテンツ配信システムにおけるコンテンツプロバイダと、ログ収集サーバ間の処理を示すフロー図である。

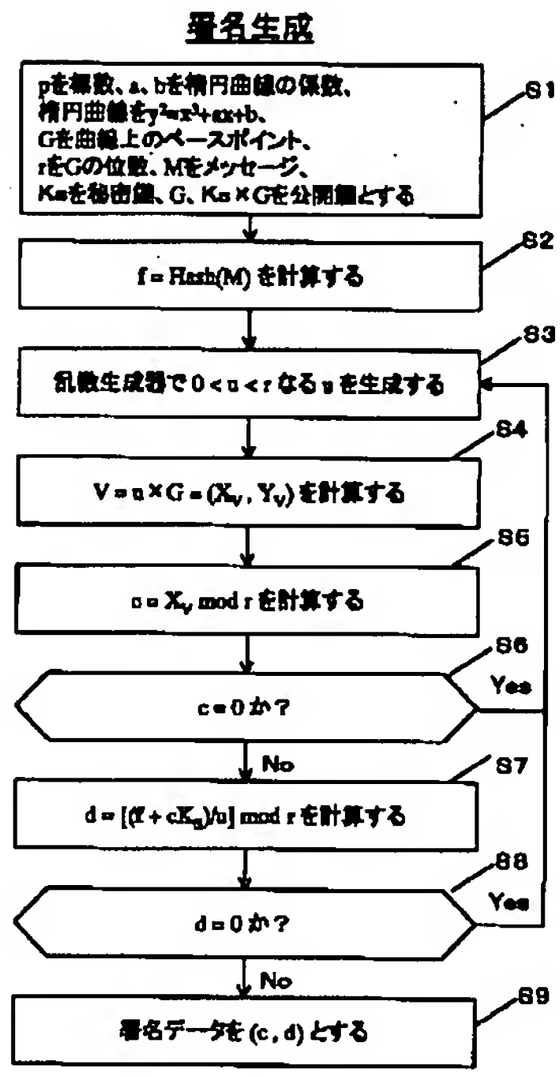
【図６４】本発明のコンテンツ配信システムにおけるショップサーバと、ログ収集サーバ間の処理を示すフロー図である。
【図６５】本発明のコンテンツ配信システムにおけるショップサーバと、ログ収集サーバ間の処理を示すフロー図である。
【図６６】本発明のコンテンツ配信システムにおいて適用される属性情報について説明する図である。
【図６７】本発明のコンテンツ配信システムにおいて適用可能な属性情報を持つ公開鍵証明書構成を示す図である。
【図６８】本発明のコンテンツ配信システムにおいて適用可能な公開鍵証明書および属性証明書構成を示す図である。
【図６９】本発明のコンテンツ配信システムにおける公開鍵証明書の新規発行処理を説明する図である。
【図７０】本発明のコンテンツ配信システムにおける公開鍵証明書の更新処理を説明する図である。
【図７１】本発明のコンテンツ配信システムにおける属性証明書の新規発行処理を説明する図である。
【図７２】本発明のコンテンツ配信システムにおける属性チェックを伴うコンテンツ配信処理を説明する図である。
【図７３】本発明のコンテンツ配信システムにおける属性チェックを伴う相互認証処理を説明するフロー図である。
【図７４】本発明のコンテンツ配信システムにおける属性チェックを伴うコンテンツ配信処理を説明する図である。
【図７５】本発明のコンテンツ配信システムにおける属性チェックを伴うデータ検証処理を説明するフロー図である。
【図７６】本発明のコンテンツ配信システムにおける属性チェックを伴うデータ検証処理を説明するフロー図である。
【符号の説明】
１００　ショップサーバ
１１０　コンテンツデータベース
１２０　購買管理データベース
１３０　制御手段
１３１　制御部
１３２　ＲＯＭ
１３３　ＲＡＭ
１３４　表示部
１３５　入力部
１３６　ＨＤＤ
１３７　ドライブ
１３８　ネットワークインタフェース
２００　ユーザ機器
２２０　購入管理データベース
２３０　制御手段
３００　ユーザ機器認証サーバ
３２０　ライセンス管理データベース
３３０　制御手段
４００　配信サーバ
４１０　コンテンツデータベース
６１０　チケット発行サーバ
６１２　購買管理データベース
６１３　制御手段
６２０　ユーザ機器
６３０　ユーザ機器認証サーバ
６４０　配信サーバ
６４２　配信管理データベース
６４３　制御手段
６４４　コンテンツデータベース
６５０　チケット換金サーバ
６５２　チケット換金管理データベース
６５３　制御手段
８０１　チケット発行体
８０２　ユーザ機器
８０３　ライセンスホルダ
８０４　コンテンツ制作者
８０５　銀行
９０１　ショップサーバ
９０２　ユーザ機器
９０３　ログ収集サーバ
９０４　オーサリングサーバ
９０５　コンテンツプロバイダ
９０３１　ログ管理データベース
９０３２　制御手段
１０１０　ショップサーバ
１０２０　ユーザ機器
１０３０　サービス運営体
１０４０　公開鍵証明書発行局
１０５０　属性証明書発行局

【図１】



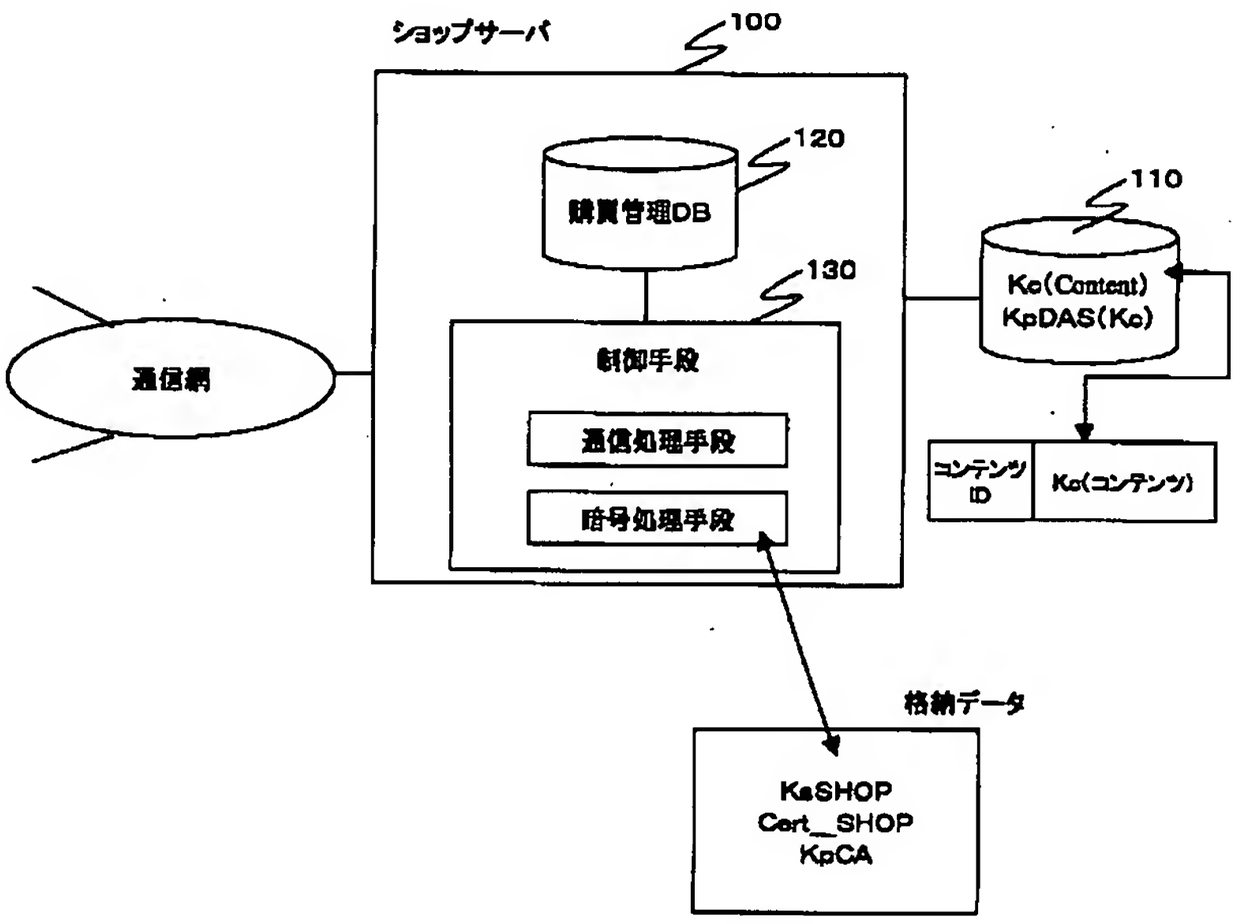
【図２】

【図１０】



署名生成(IEEE P1363/D13)

【図２】



【図６】

ユーザ機器認証サーバ処理No.	機器ID	トランザクションID	コンテンツID	ショップID	ショップ処理No.	ステータス
50001	1234567890	999888777	5000	1234	10001	鍵送信完了
50002	2345678901	666555444	4050	1234	10002	鍵かけかえ完了

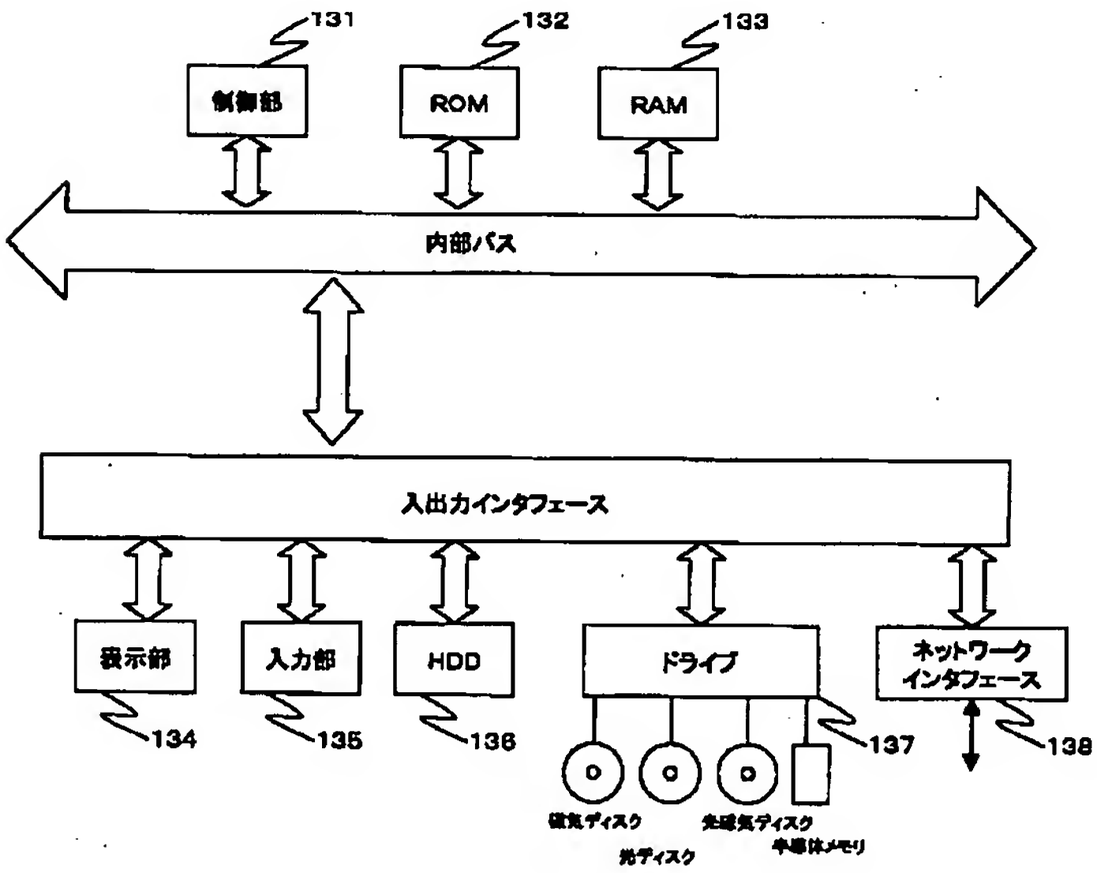
ユーザ機器認証サーバ・ライセンス管理DB

【図３】

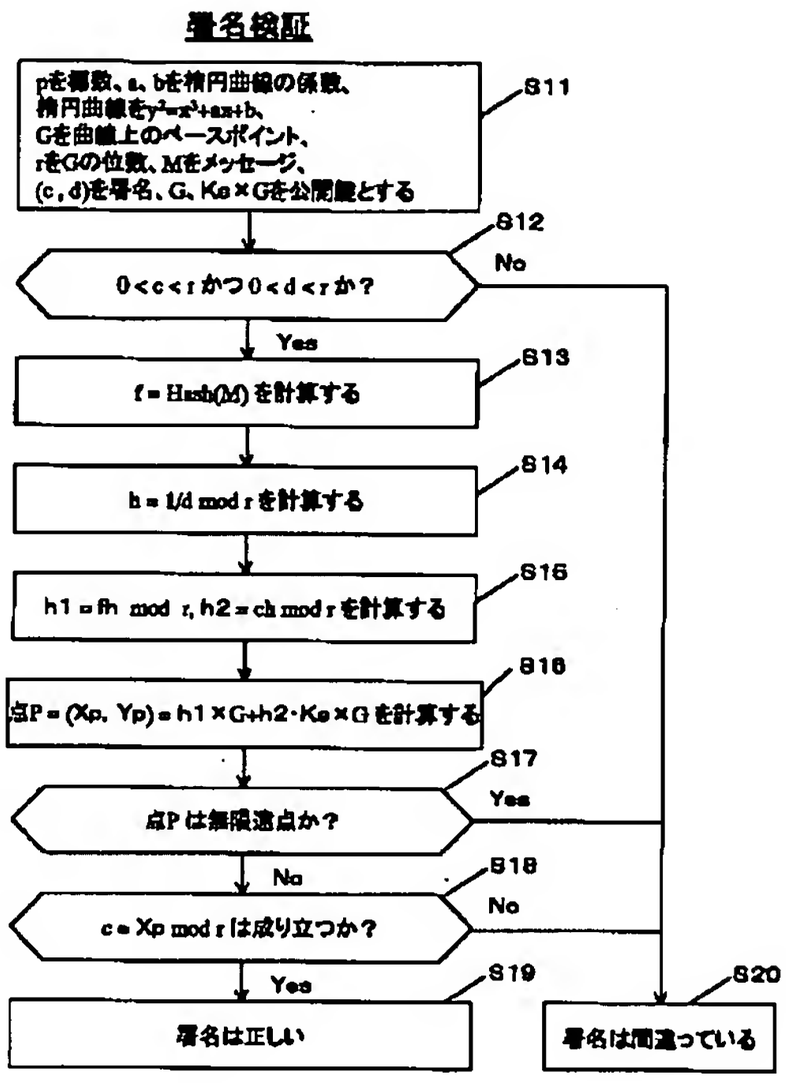
ショップ処理No.	機器ID	トランザクションID	コンテンツID	ステータス
10001	1234567890	999888777	5000	鍵2配信完了
10002	2345678901	666555444	4050	課金完了
10003	3456789012	333222111	1000	暗号化コンテンツ鍵送信要求受付完了
10004	4567890123	000999888	3000	鍵受信完了
10005	5678901234	777666555	5050	鍵1配信完了
10006	6789012345	444333222	2050	購入受付完了

ショップサーバ・購買管理DB

【図４】



【図１１】



署名検証(IEEE P1363/D13)

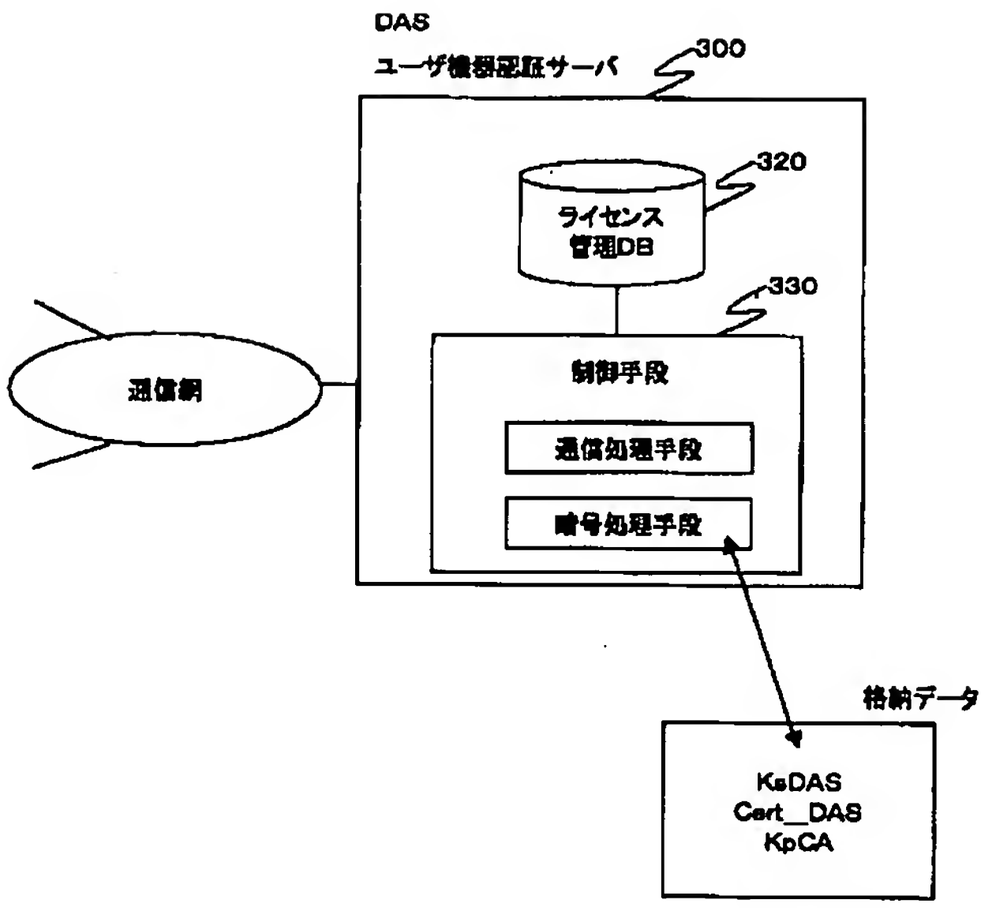
【図８】

機器ID:1234567890

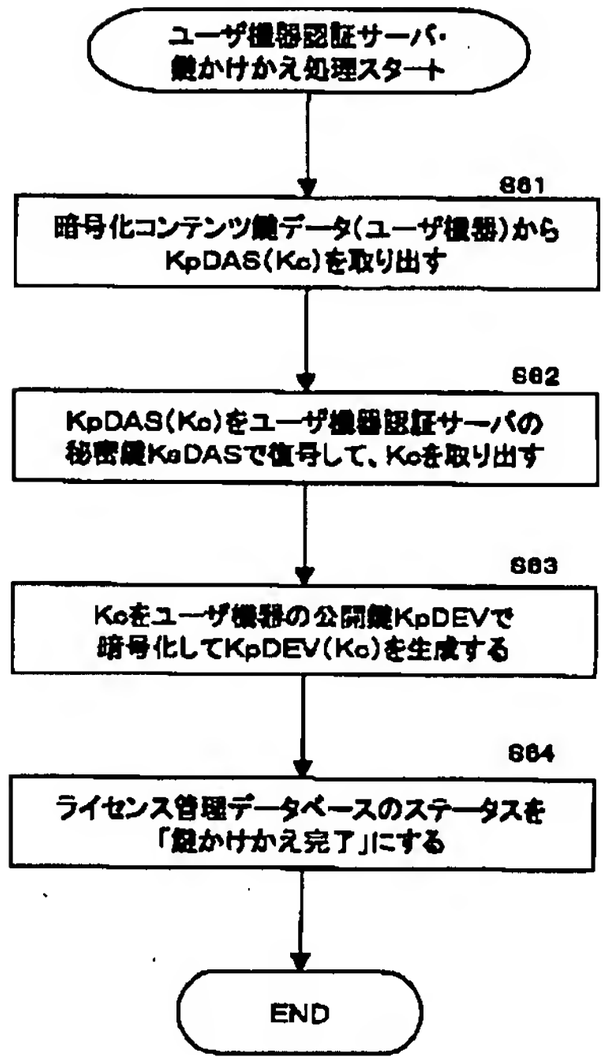
トランザクションID	コンテンツID	ショップID	ステータス
999888777	5000	1234	鍵2受信完了
666555444	4050	9876	購入要求送信完了

ユーザ機器・購入管理DB

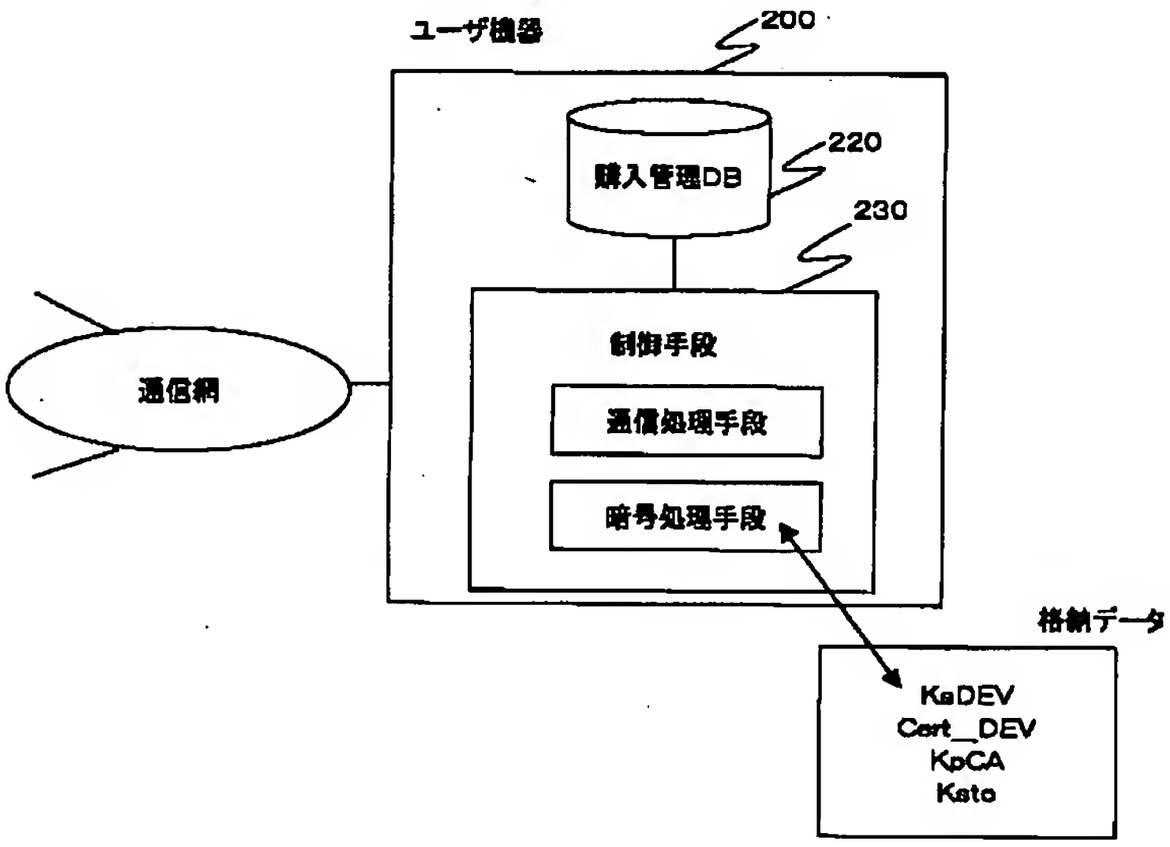
【図５】


DAS
ユーザ機器認証サーバ
300
320
ライセンス
管理DB
330
制御手段
通信処理手段
暗号処理手段
通信網
格納データ
KsDAS
Cert_DAS
KpCA

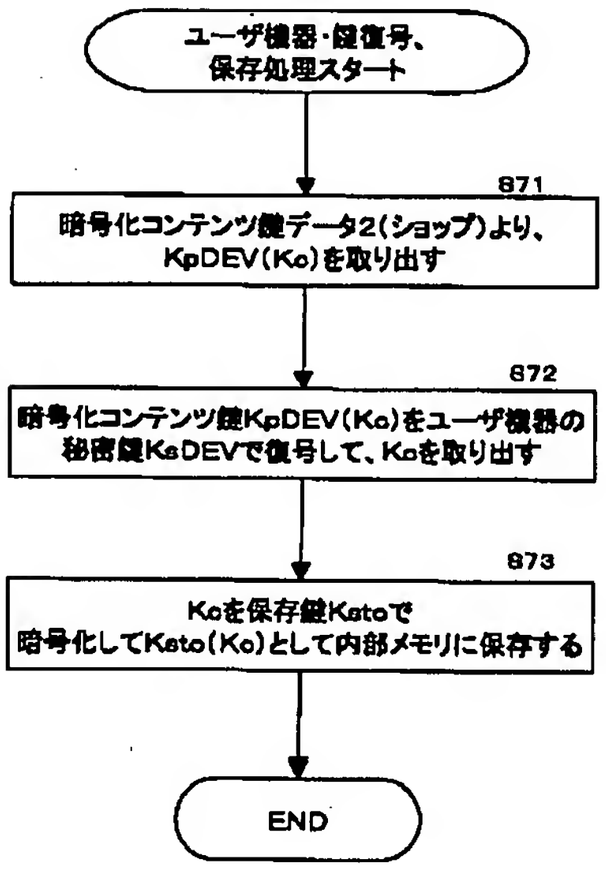
【図１６】


ユーザ機器認証サーバ・
鍵かけかえ処理スタート
S61
暗号化コンテンツ鍵データ(ユーザ機器)から
KpDAS(Ko)を取り出す
S62
KpDAS(Ko)をユーザ機器認証サーバの
秘密鍵KsDASで復号して、Koを取り出す
S63
Koをユーザ機器の公開鍵KpDEVで
暗号化してKpDEV(Ko)を生成する
S64
ライセンス管理データベースのステータスを
「鍵かけかえ完了」にする
END

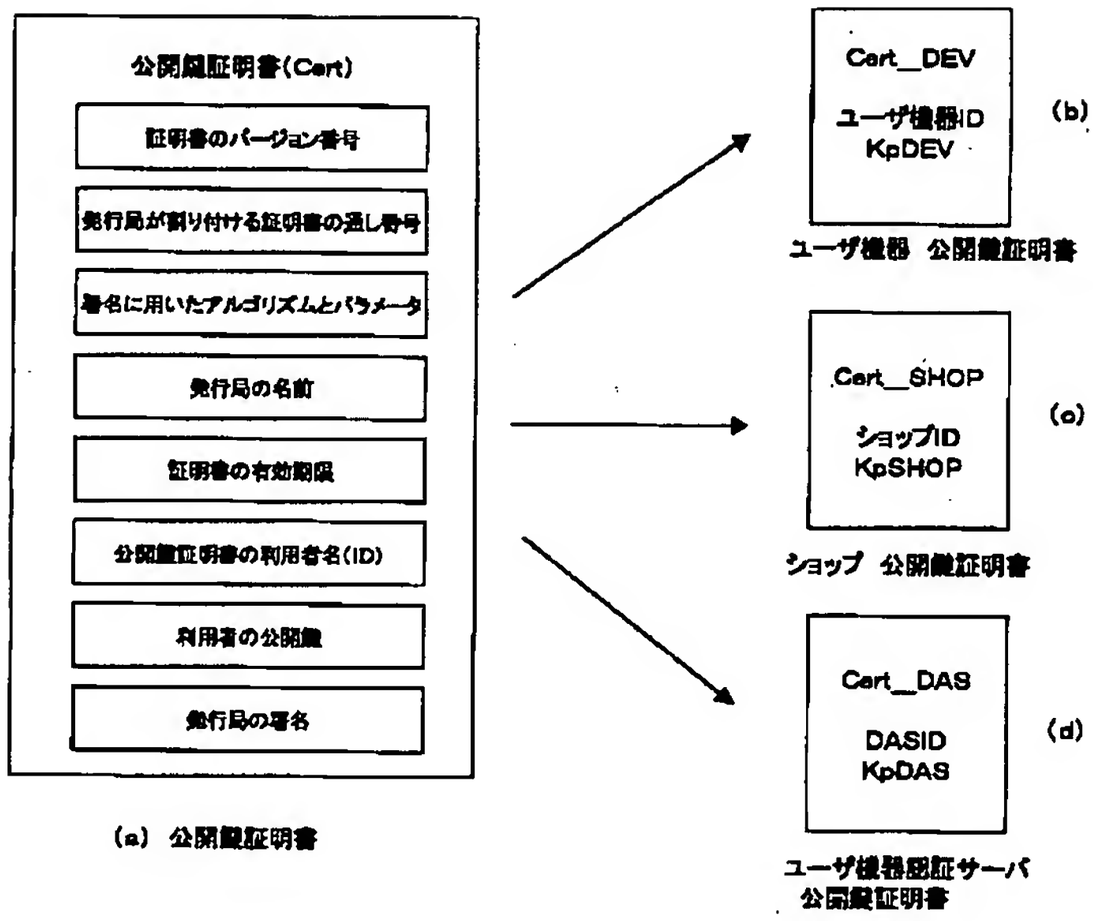
【図７】


ユーザ機器
200
220
購入管理DB
230
制御手段
通信処理手段
暗号処理手段
通信網
格納データ
KsDEV
Cert_DEV
KpCA
Ksto

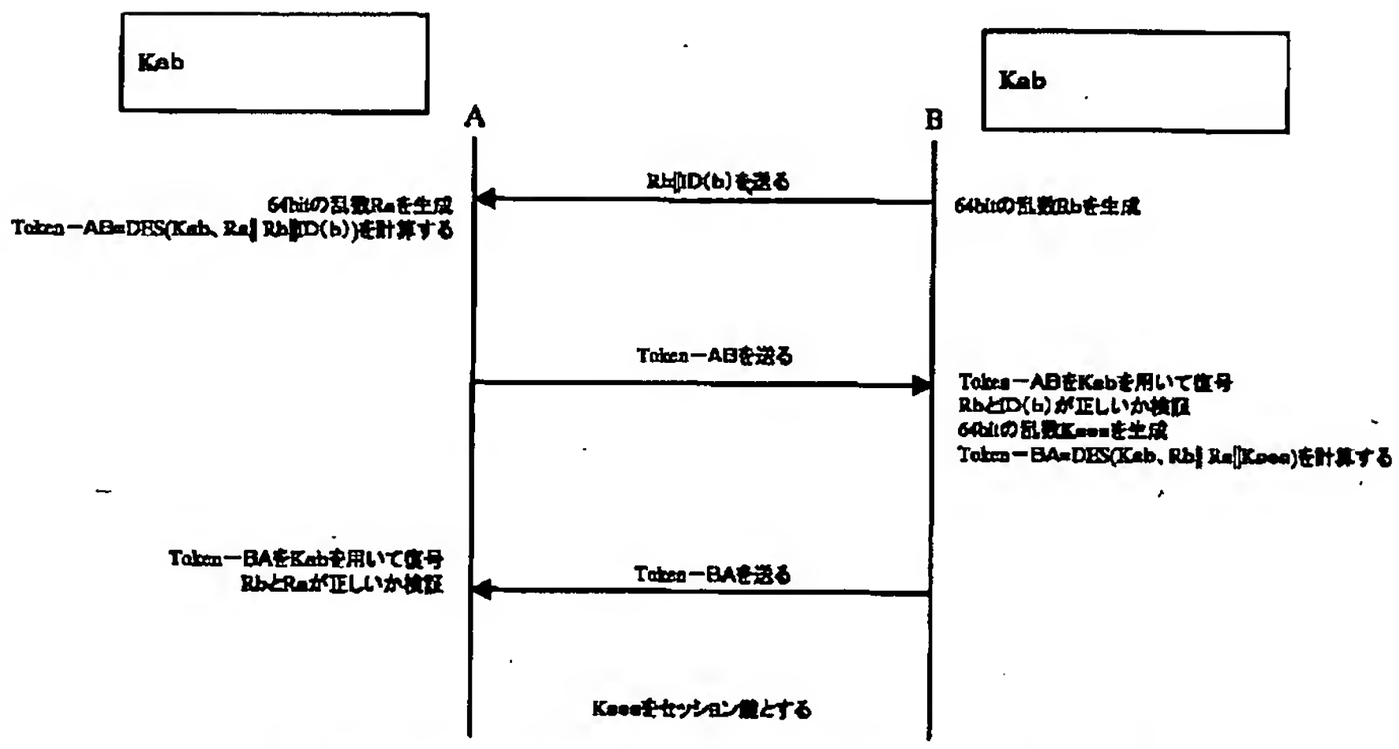
【図１９】


ユーザ機器・鍵復号、
保存処理スタート
S71
暗号化コンテンツ鍵データ2(ショップ)より、
KpDEV(Ko)を取り出す
S72
暗号化コンテンツ鍵KpDEV(Ko)をユーザ機器の
秘密鍵KsDEVで復号して、Koを取り出す
S73
Koを保存鍵Kstoで
暗号化してKsto(Ko)として内部メモリに保存する
END

【図９】

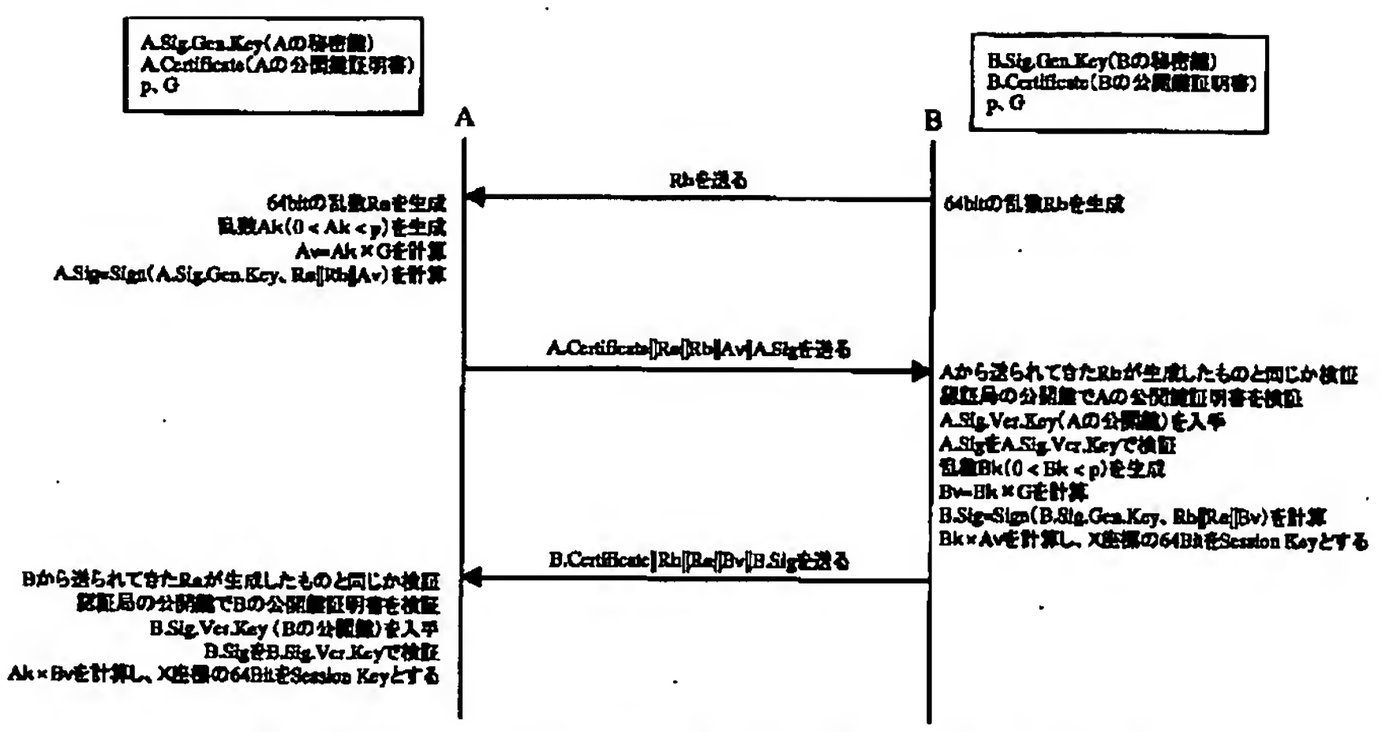


【図１２】



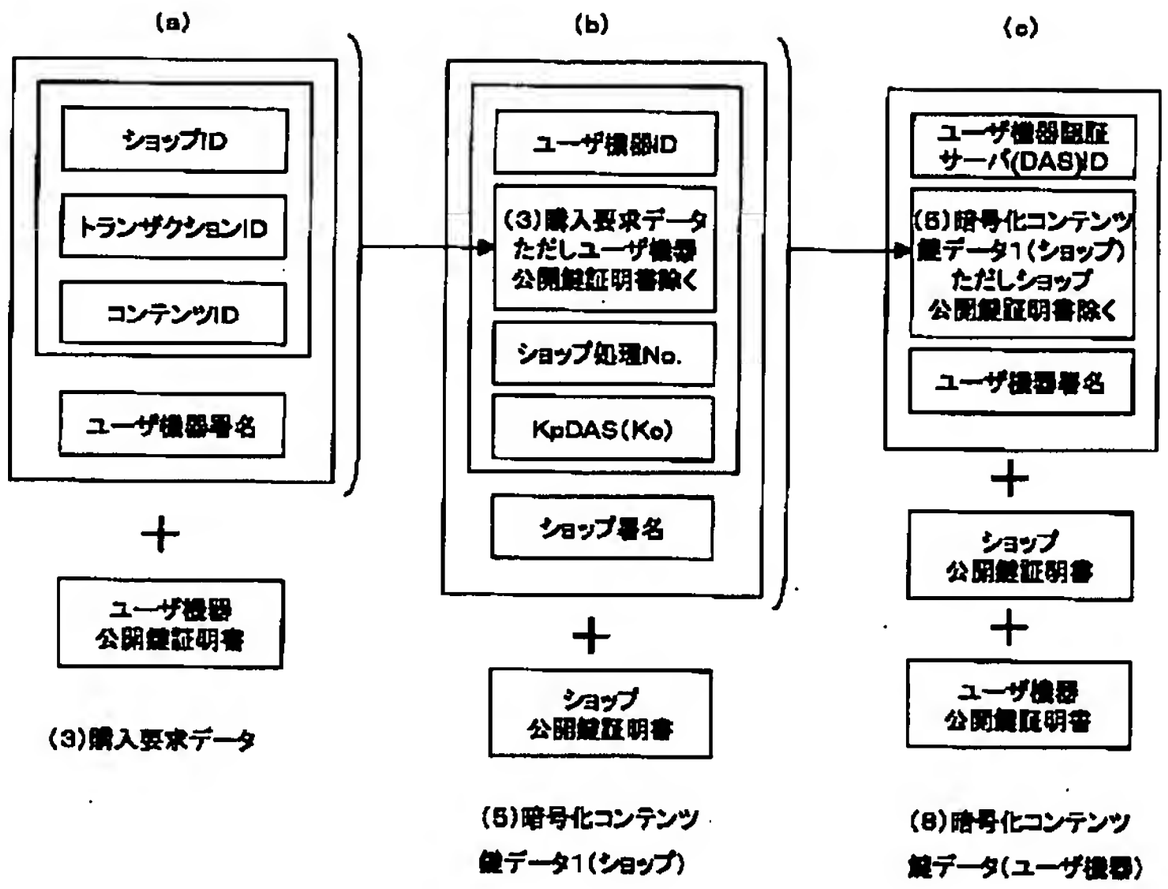
ISO/IEC 9798-2 対称鍵暗号技術を用いた相互認証および鍵共有方式

【図１３】

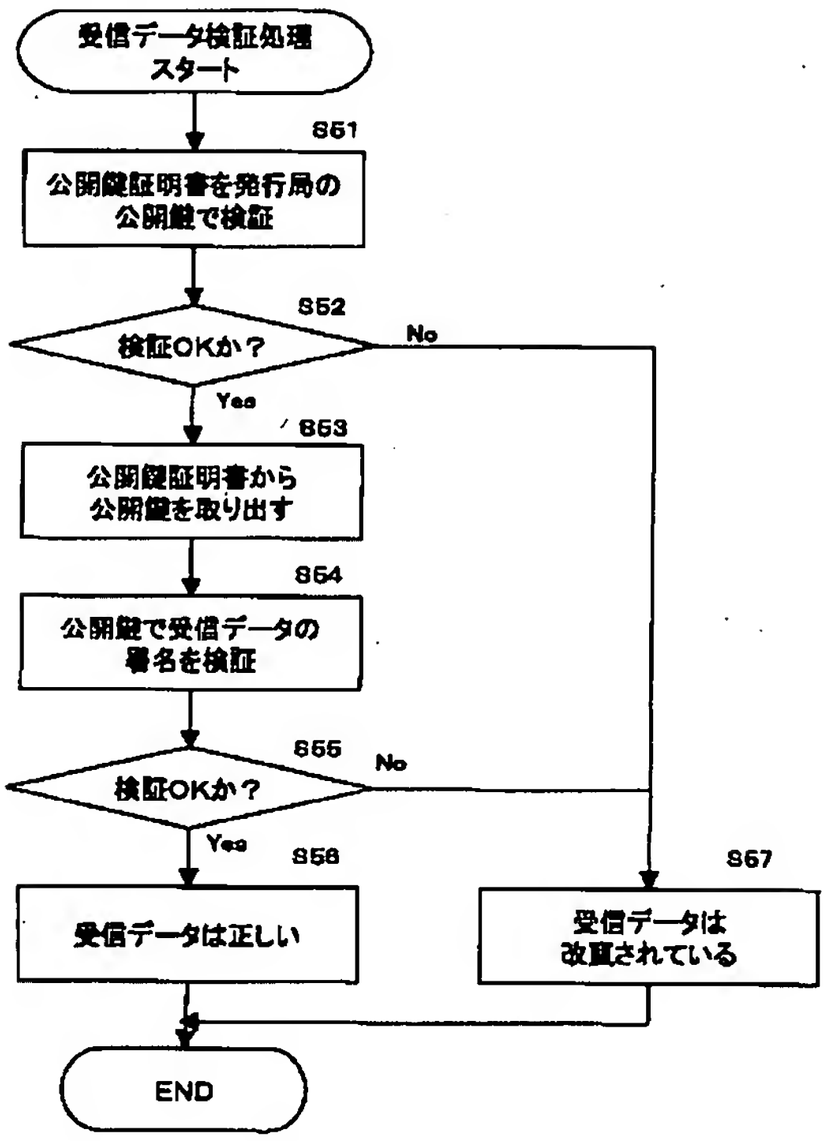


ISO/IEC 9798-3　非対称鍵暗号技術を用いた相互認証および鍵共有方式

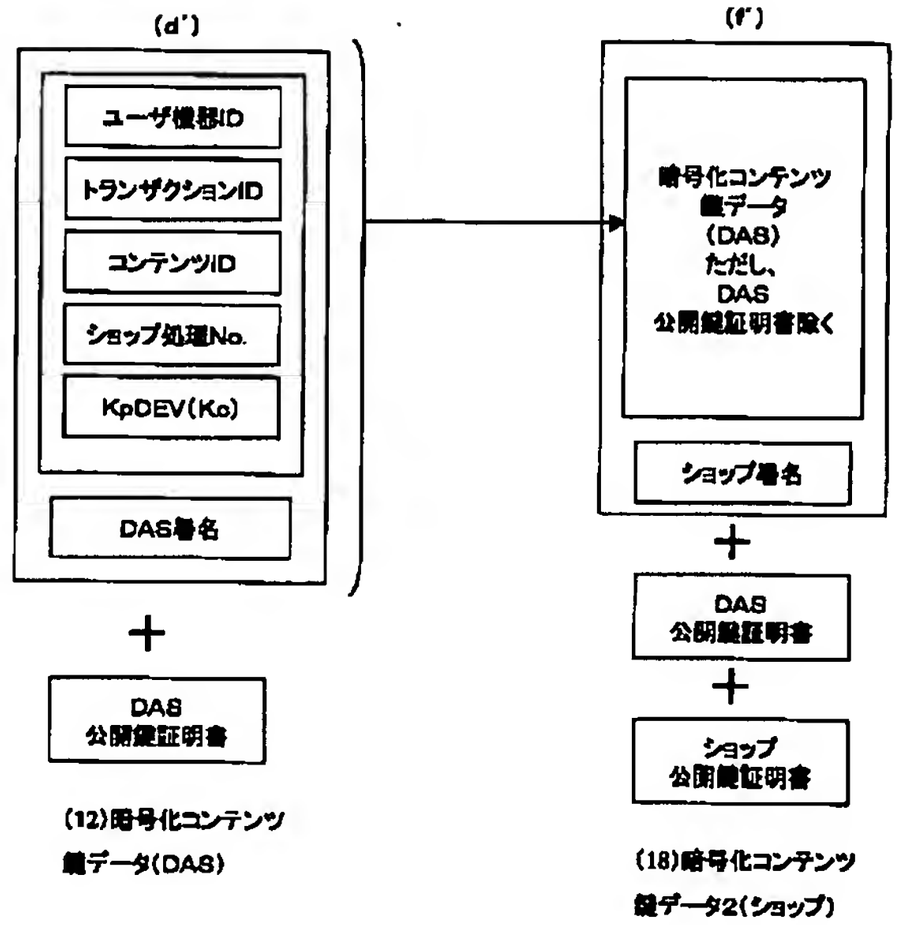
【図１４】



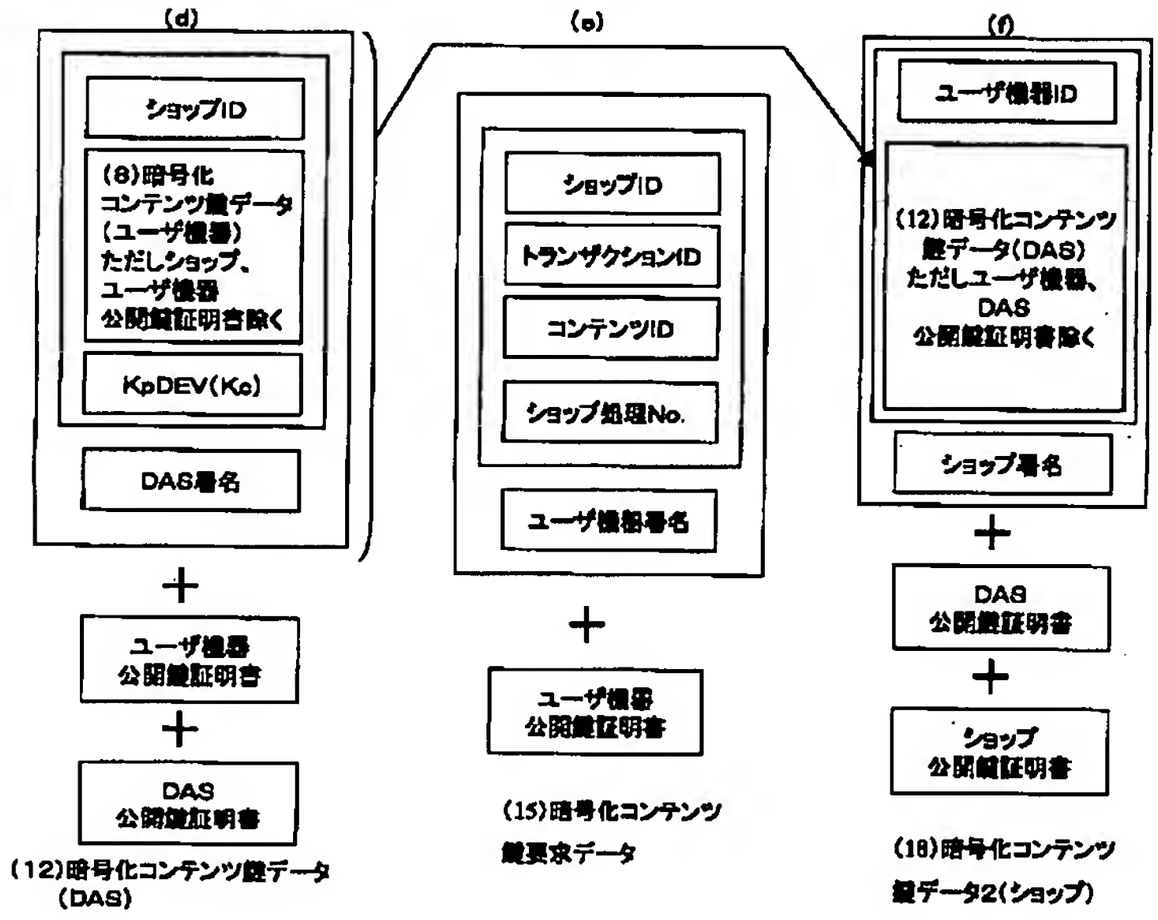
【図１５】


受信データ検証処理
スタート
S51
公開鍵証明書を発行局の
公開鍵で検証
S52
検証OKか？
No
Yes
S53
公開鍵証明書から
公開鍵を取り出す
S54
公開鍵で受信データの
署名を検証
S55
検証OKか？
No
Yes
S56
受信データは正しい
S57
受信データは
改竄されている
END

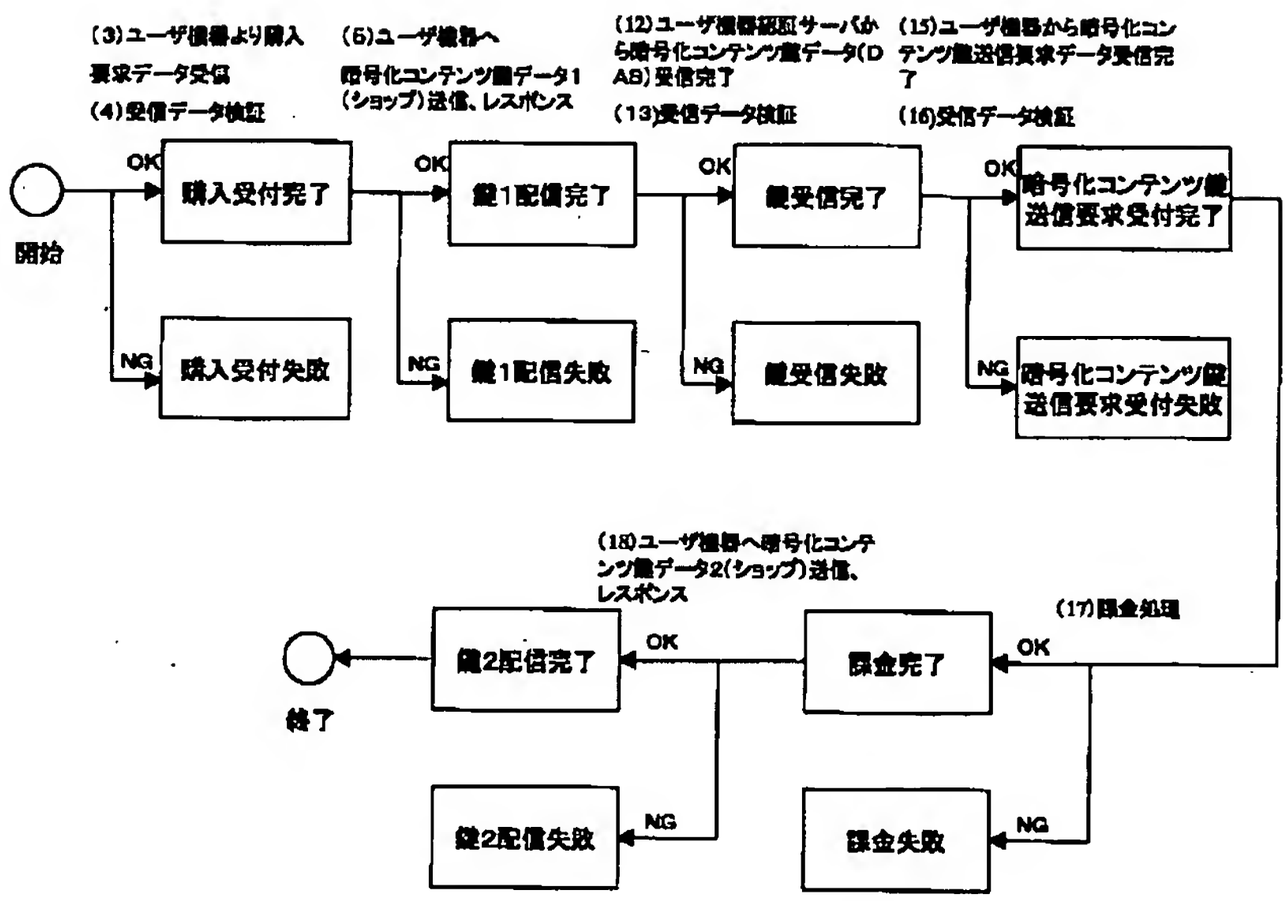
【図１８】


(d')
ユーザ機器ID
トランザクションID
コンテンツID
ショップ処理No.
KpDEV(Ko)
DAS署名
+
DAS
公開鍵証明書
(12)暗号化コンテンツ
鍵データ(DAS)
(f')
暗号化コンテンツ
鍵データ
(DAS)
ただし、
DAS
公開鍵証明書除く
ショップ署名
+
DAS
公開鍵証明書
+
ショップ
公開鍵証明書
(18)暗号化コンテンツ
鍵データ2(ショップ)

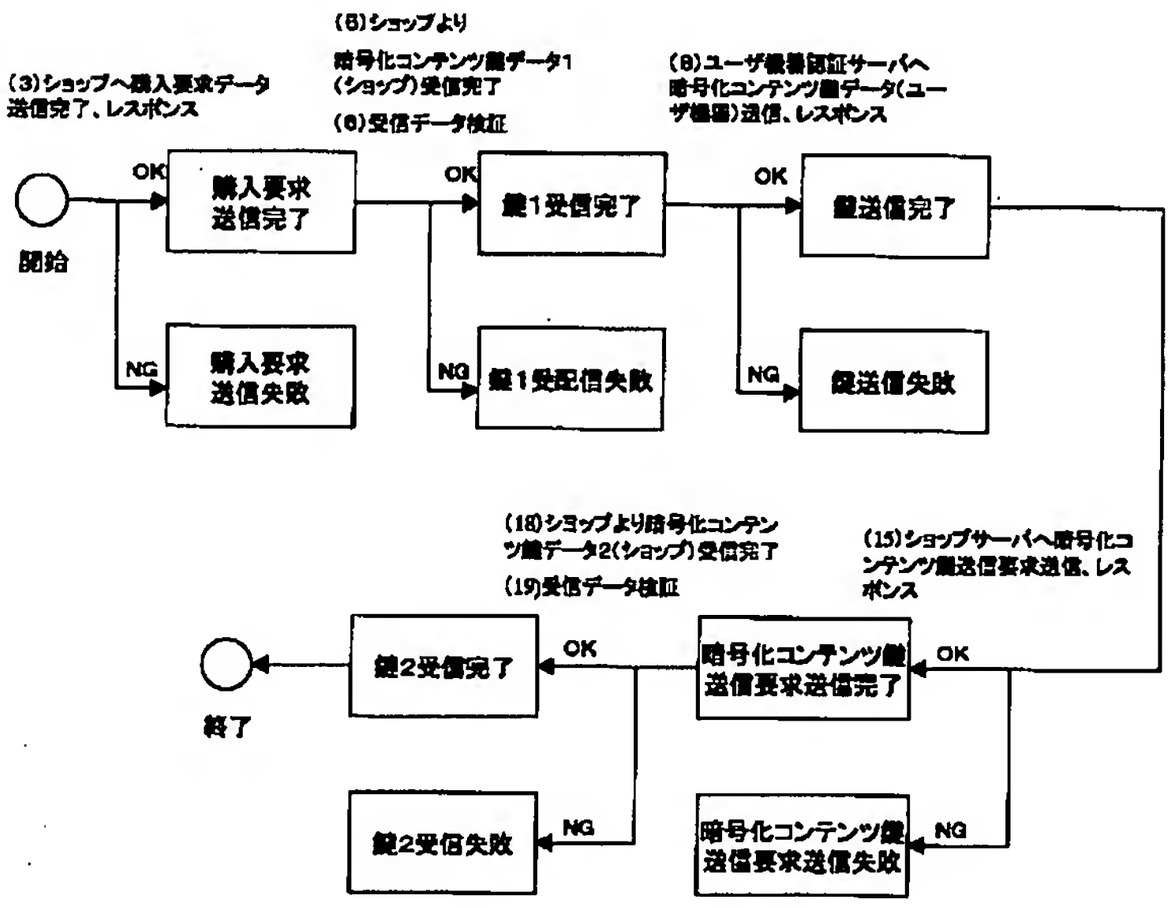
【図１７】


(d)
ショップID
(8)暗号化
コンテンツ鍵データ
(ユーザ機器)
ただしショップ、
ユーザ機器
公開鍵証明書除く
KpDEV(Ko)
DAS署名
+
ユーザ機器
公開鍵証明書
+
DAS
公開鍵証明書
(12)暗号化コンテンツ鍵データ
(DAS)
(e)
ショップID
トランザクションID
コンテンツID
ショップ処理No.
ユーザ機器署名
+
ユーザ機器
公開鍵証明書
(15)暗号化コンテンツ
鍵要求データ
(f)
ユーザ機器ID
(12)暗号化コンテンツ
鍵データ(DAS)
ただしユーザ機器、
DAS
公開鍵証明書除く
ショップ署名
+
DAS
公開鍵証明書
+
ショップ
公開鍵証明書
(18)暗号化コンテンツ
鍵データ2(ショップ)

【図２０】



【図２１】

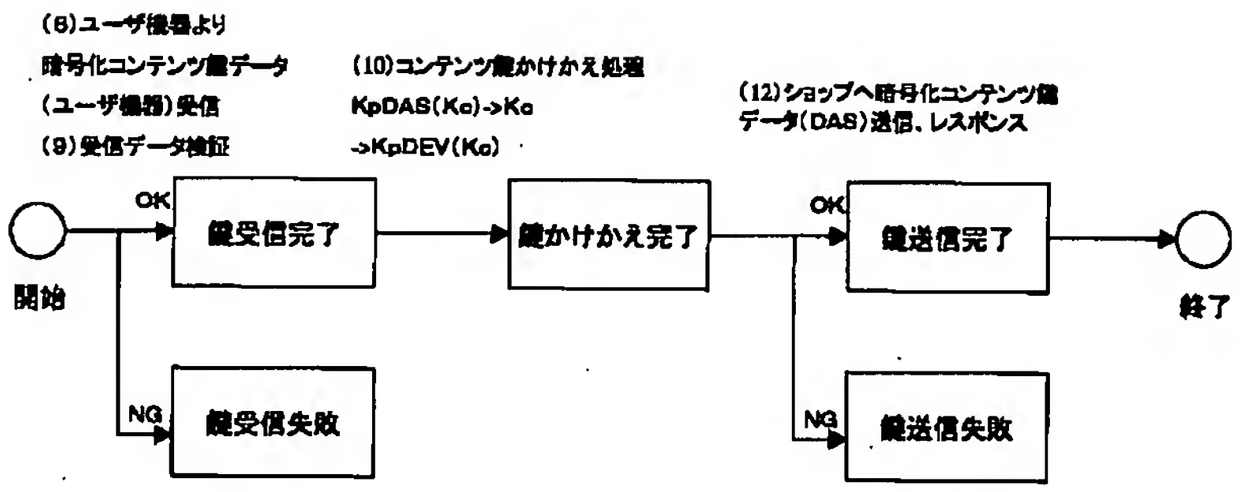


【図３９】

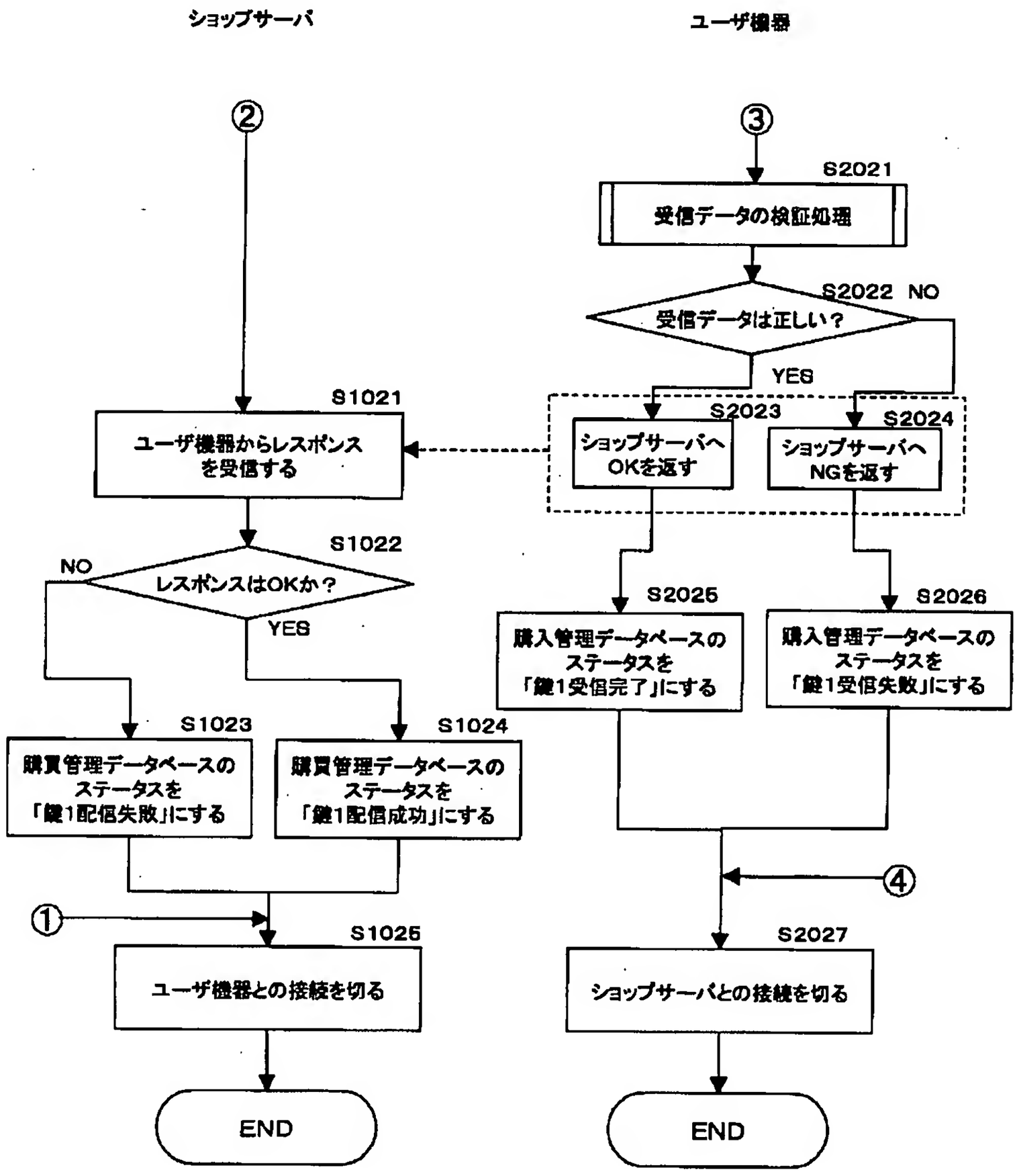
チケット発行処理No.	機器ID	トランザクションID	コンテンツID	チケット利用先ID	金額	有効期限	ステータス
10001	1234567890	999888777	5000	222331234	¥1000	00/04/01	課金処理レポート受信完了
10002	2345678901	666555444	4050	223345634	¥250	00/07/31	電子チケット配信完了
10003	3456788901	321655444	4021	345645234	¥800	00/07/31	購入受付完了

チケット発行サーバ・チケット発行管理DB

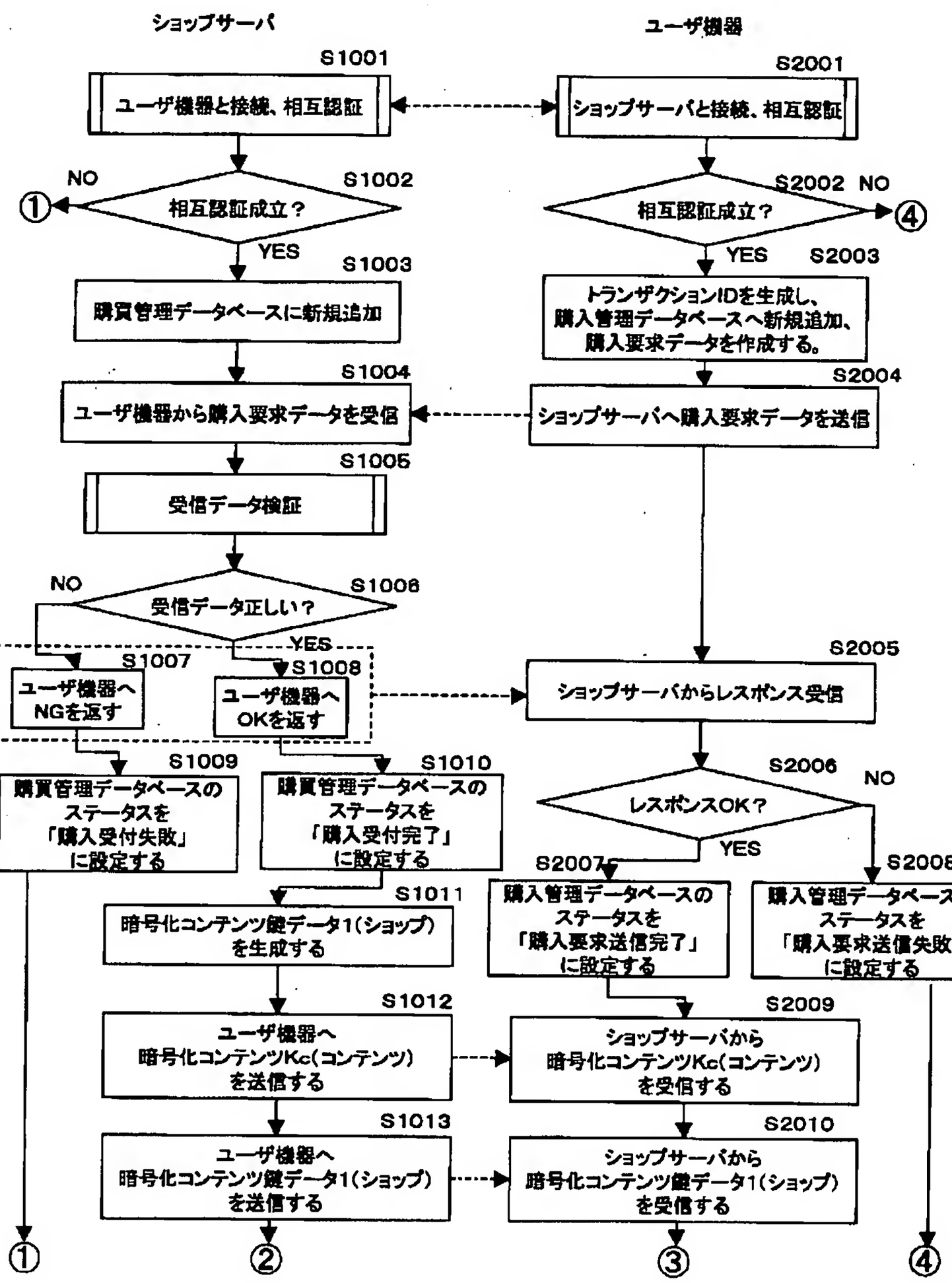
【図２２】


(6)ユーザ機器より
暗号化コンテンツ鍵データ
(ユーザ機器)受信
(9)受信データ検証
(10)コンテンツ鍵かけかえ処理
KpDAS(Ko)->Ko
->KpDEV(Ko)
(12)ショップへ暗号化コンテンツ鍵
データ(DAS)送信、レスポンス
OK
鍵受信完了
鍵かけかえ完了
OK
鍵送信完了
開始
終了
NG
鍵受信失敗
NG
鍵送信失敗

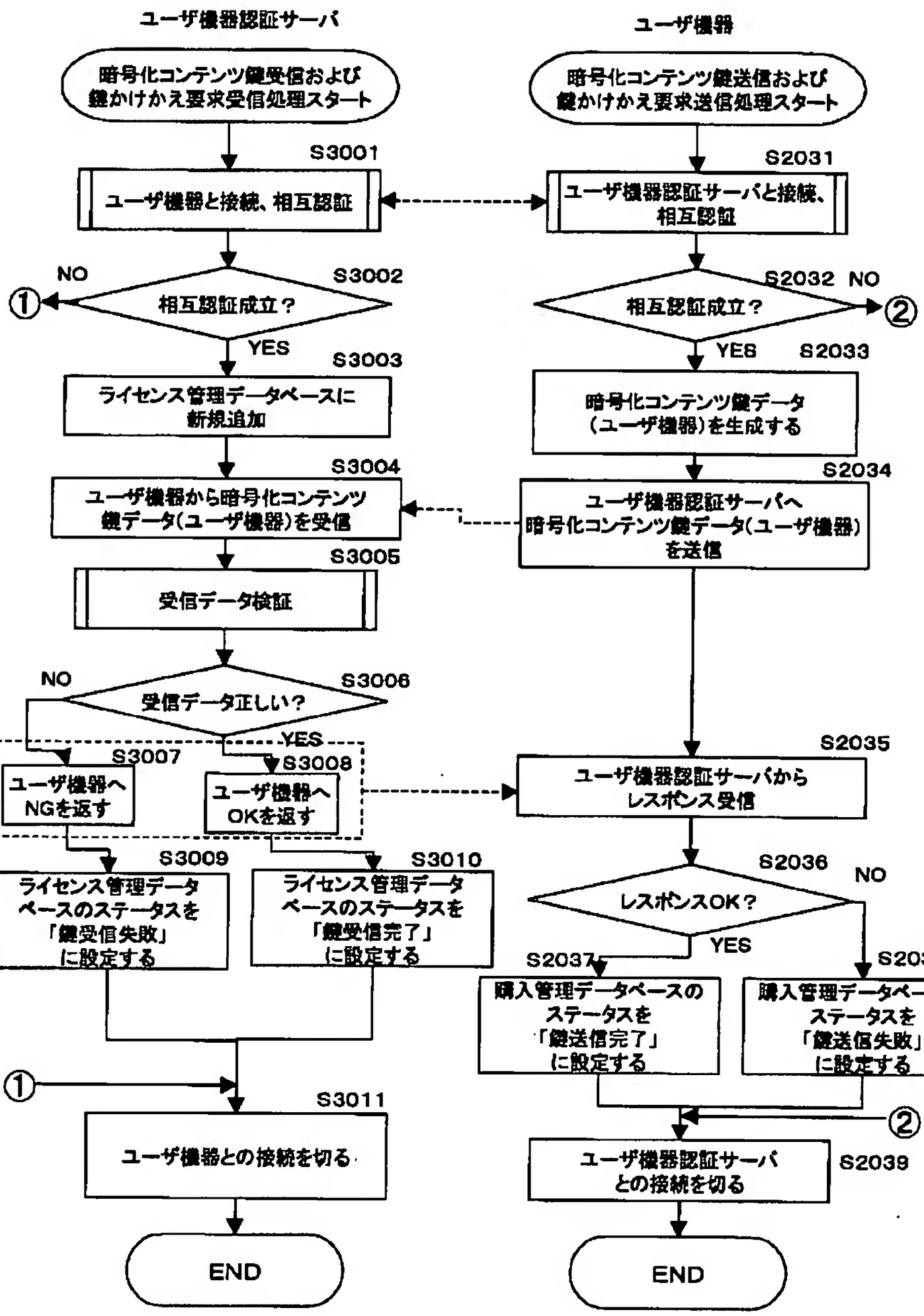
【図２４】


ショップサーバ
ユーザ機器
②
③
S2021
受信データの検証処理
S2022 NO
受信データは正しい？
YES
S1021
S2023
S2024
ユーザ機器からレスポンス
を受信する
ショップサーバへ
OKを返す
ショップサーバへ
NGを返す
S1022
NO
レスポンスはOKか？
YES
S2025
S2026
購入管理データベースの
ステータスを
「鍵1受信完了」にする
購入管理データベースの
ステータスを
「鍵1受信失敗」にする
S1023
S1024
購買管理データベースの
ステータスを
「鍵1配信失敗」にする
購買管理データベースの
ステータスを
「鍵1配信成功」にする
④
①
S1025
S2027
ユーザ機器との接続を切る
ショップサーバとの接続を切る
END
END

【図２３】


ショップサーバ
ユーザ機器
S1001
ユーザ機器と接続、相互認証
S2001
ショップサーバと接続、相互認証
NO
S1002
相互認証成立？
①
YES
S1003
購買管理データベースに新規追加
S2002 NO
相互認証成立？
④
YES
S2003
トランザクションIDを生成し、
購入管理データベースへ新規追加、
購入要求データを作成する。
S1004
ユーザ機器から購入要求データを受信
S2004
ショップサーバへ購入要求データを送信
S1005
受信データ検証
NO
S1006
受信データ正しい？
YES
S1007
ユーザ機器へ
NGを返す
S1008
ユーザ機器へ
OKを返す
S2005
ショップサーバからレスポンス受信
S1009
購買管理データベースの
ステータスを
「購入受付失敗」
に設定する
S1010
購買管理データベースの
ステータスを
「購入受付完了」
に設定する
S2006
NO
レスポンスOK？
YES
S2007
購入管理データベースの
ステータスを
「購入要求送信完了」
に設定する
S2008
購入管理データベースの
ステータスを
「購入要求送信失敗」
に設定する
S1011
暗号化コンテンツ鍵データ1(ショップ)
を生成する
S1012
ユーザ機器へ
暗号化コンテンツKc(コンテンツ)
を送信する
S2009
ショップサーバから
暗号化コンテンツKc(コンテンツ)
を受信する
S1013
ユーザ機器へ
暗号化コンテンツ鍵データ1(ショップ)
を送信する
S2010
ショップサーバから
暗号化コンテンツ鍵データ1(ショップ)
を受信する
①
②
③
④

【図２５】

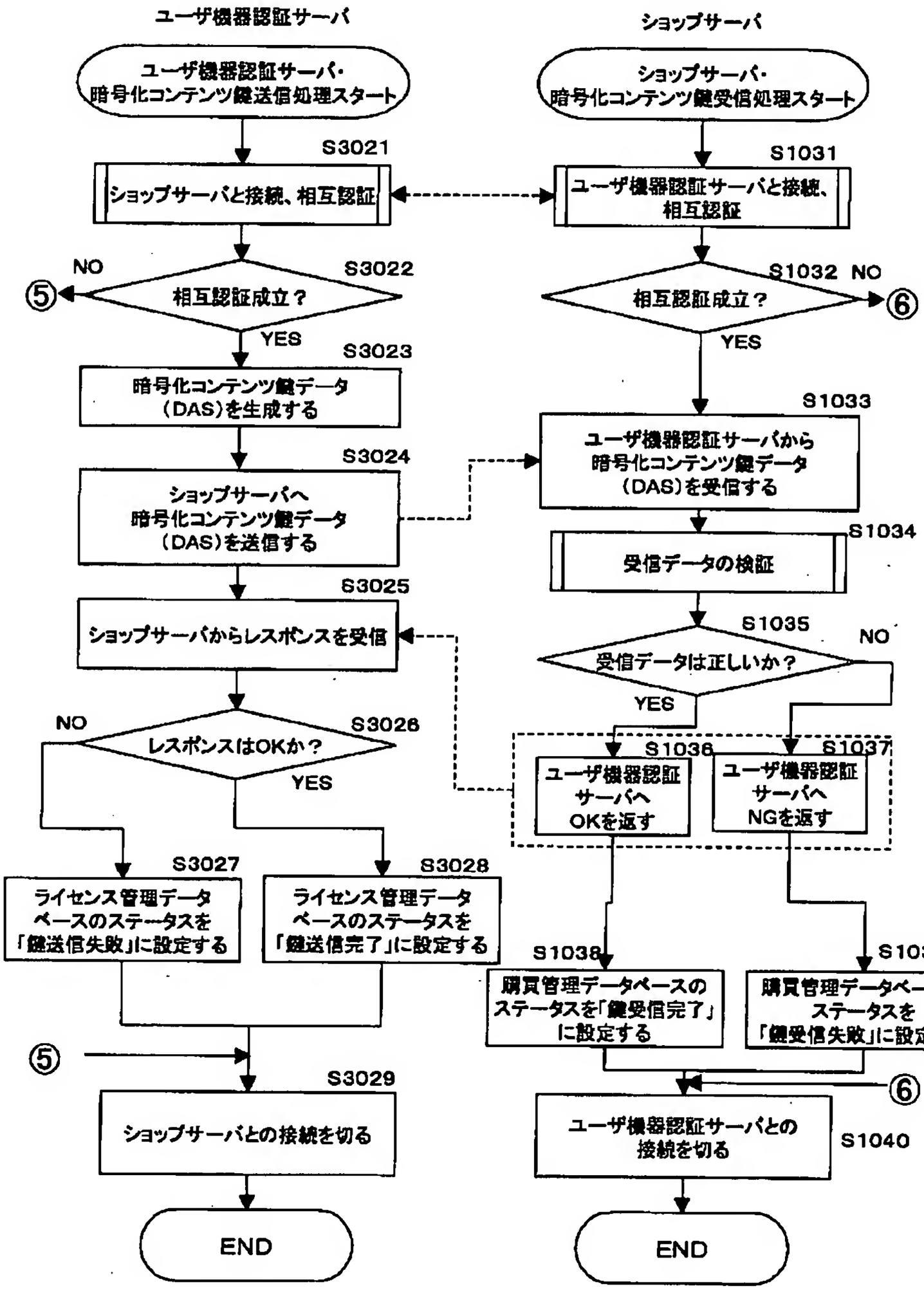


【図４５】

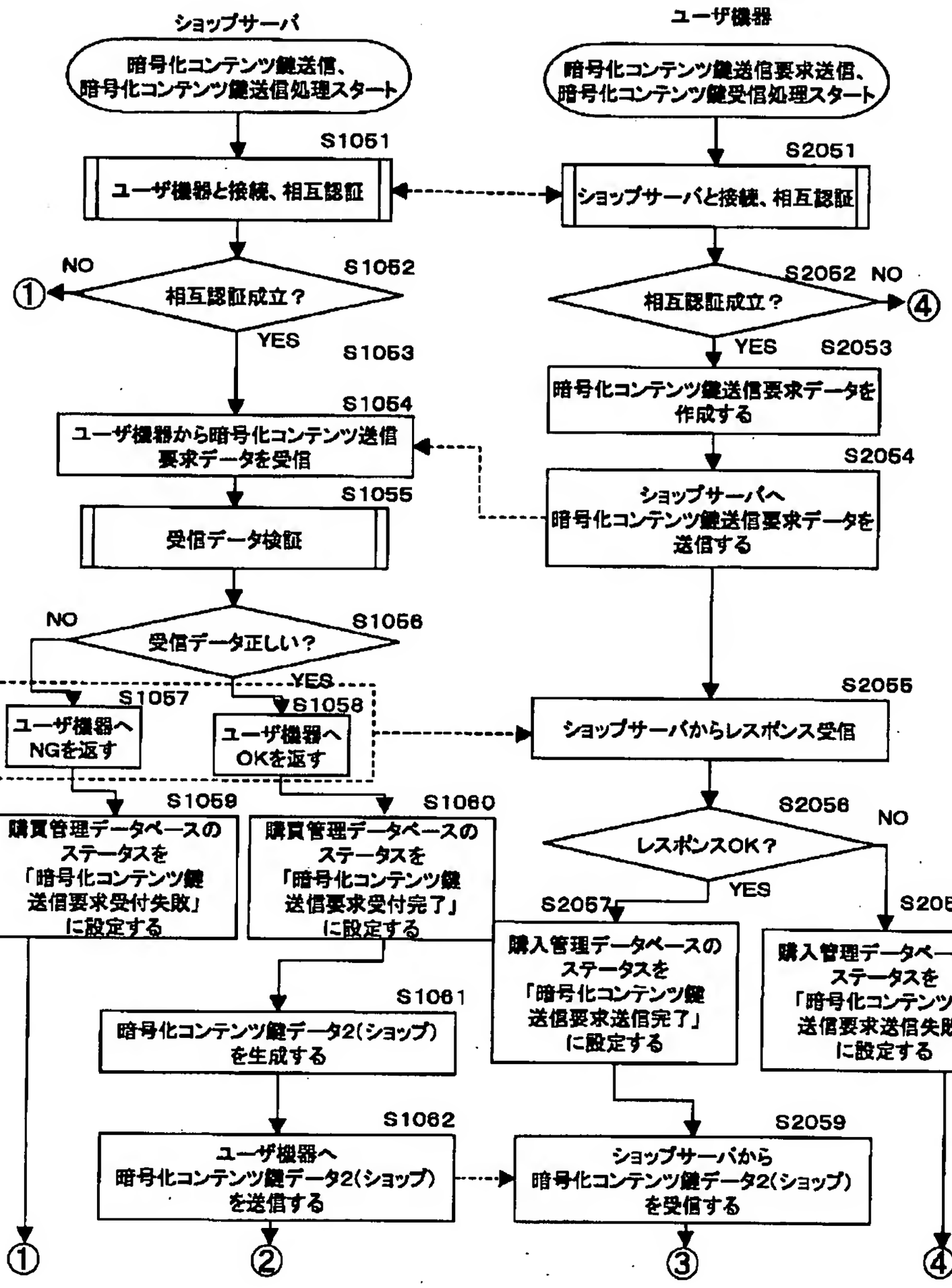
チケット換金サーバ処理No.	換金依頼元ID	チケット発行体ID	チケット発行処理No.	金額	機器ID	トランザクションID	ステータス
50001	12345	1234	10023	¥1000	1234567890	999888777	換金処理レポート送信完了
50002	23450	4455	10455	¥250	2345678901	666555444	換金処理完了
50003	33201	2354	10254	¥800	3456788901	321655444	電子チケット受信完了

チケット換金サーバ・チケット換金管理DB

【図２６】


ユーザ機器認証サーバ
ユーザ機器認証サーバ・
暗号化コンテンツ鍵送信処理スタート
S3021
ショップサーバと接続、相互認証
NO
S3022
相互認証成立？
⑤
YES
S3023
暗号化コンテンツ鍵データ
（DAS）を生成する
S3024
ショップサーバへ
暗号化コンテンツ鍵データ
（DAS）を送信する
S3025
ショップサーバからレスポンスを受信
NO
S3026
レスポンスはOKか？
YES
S3027
ライセンス管理データ
ベースのステータスを
「鍵送信失敗」に設定する
S3028
ライセンス管理データ
ベースのステータスを
「鍵送信完了」に設定する
⑤
S3029
ショップサーバとの接続を切る
END
ショップサーバ
ショップサーバ・
暗号化コンテンツ鍵受信処理スタート
S1031
ユーザ機器認証サーバと接続、
相互認証
S1032
NO
相互認証成立？
⑥
YES
S1033
ユーザ機器認証サーバから
暗号化コンテンツ鍵データ
（DAS）を受信する
S1034
受信データの検証
S1035
NO
受信データは正しいか？
YES
S1036
ユーザ機器認証
サーバへ
OKを返す
S1037
ユーザ機器認証
サーバへ
NGを返す
S1038
購買管理データベースの
ステータスを「鍵受信完了」
に設定する
S1039
購買管理データベースの
ステータスを
「鍵受信失敗」に設定する
⑥
S1040
ユーザ機器認証サーバとの
接続を切る
END

【図２７】

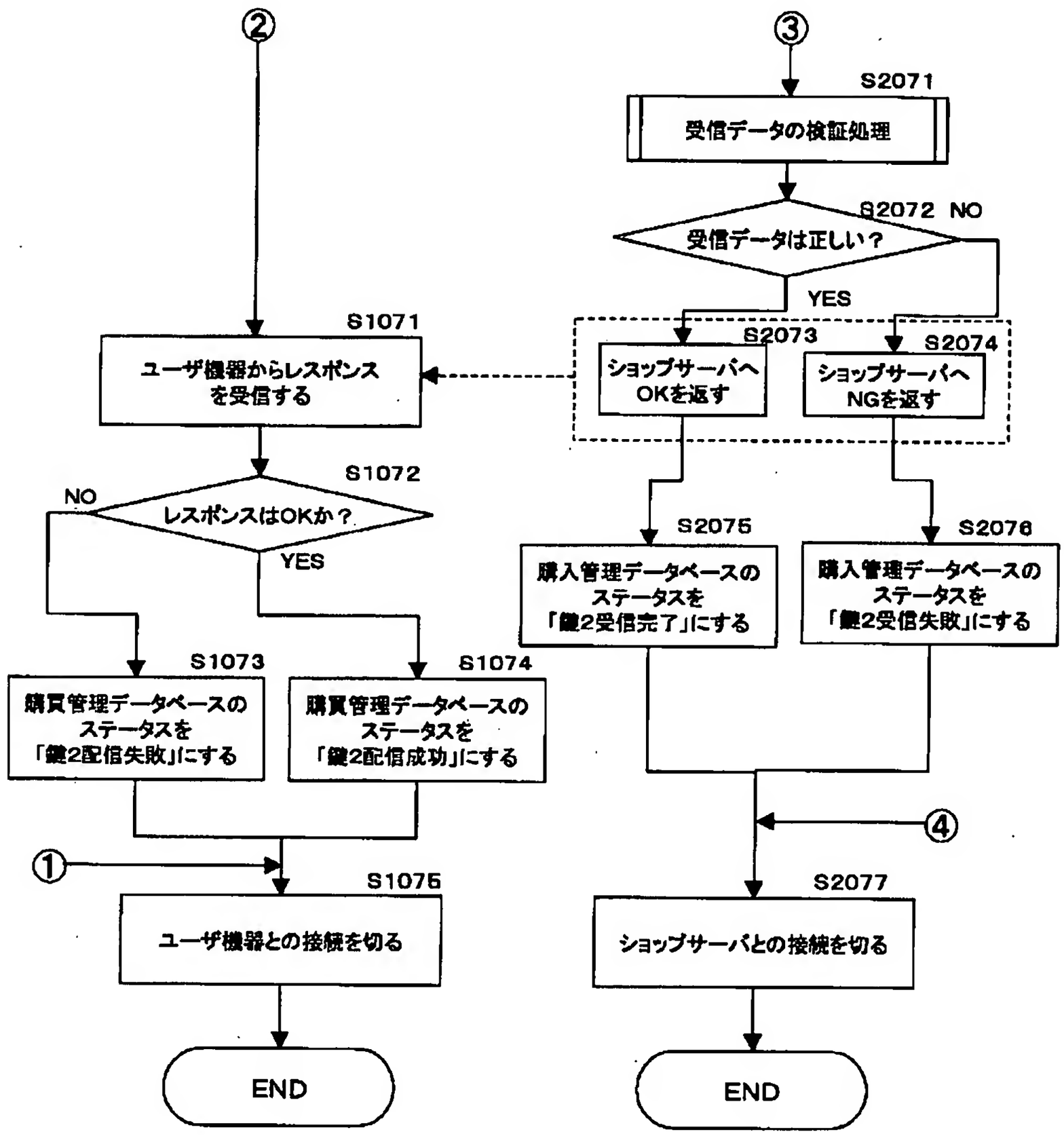


【図４３】

配信サーバ処理No.	コンテンツID	機器ID	チケット発行体ID	チケット発行処理No.	ステータス
999888777	5000	1234567890	1234	12345	換金処理レポート受信完了
666555444	4050	3427781534	2345	23456	チケット換金要求送信完了
999888779	5010	2355643551	1545	22335	配信完了
333555444	4320	4987390989	1030	32423	電子チケット受信完了
2133545445	3232	3542416759	2253	44323	電子チケット受信完了

配信サーバ-配信管理DB

【図２８】

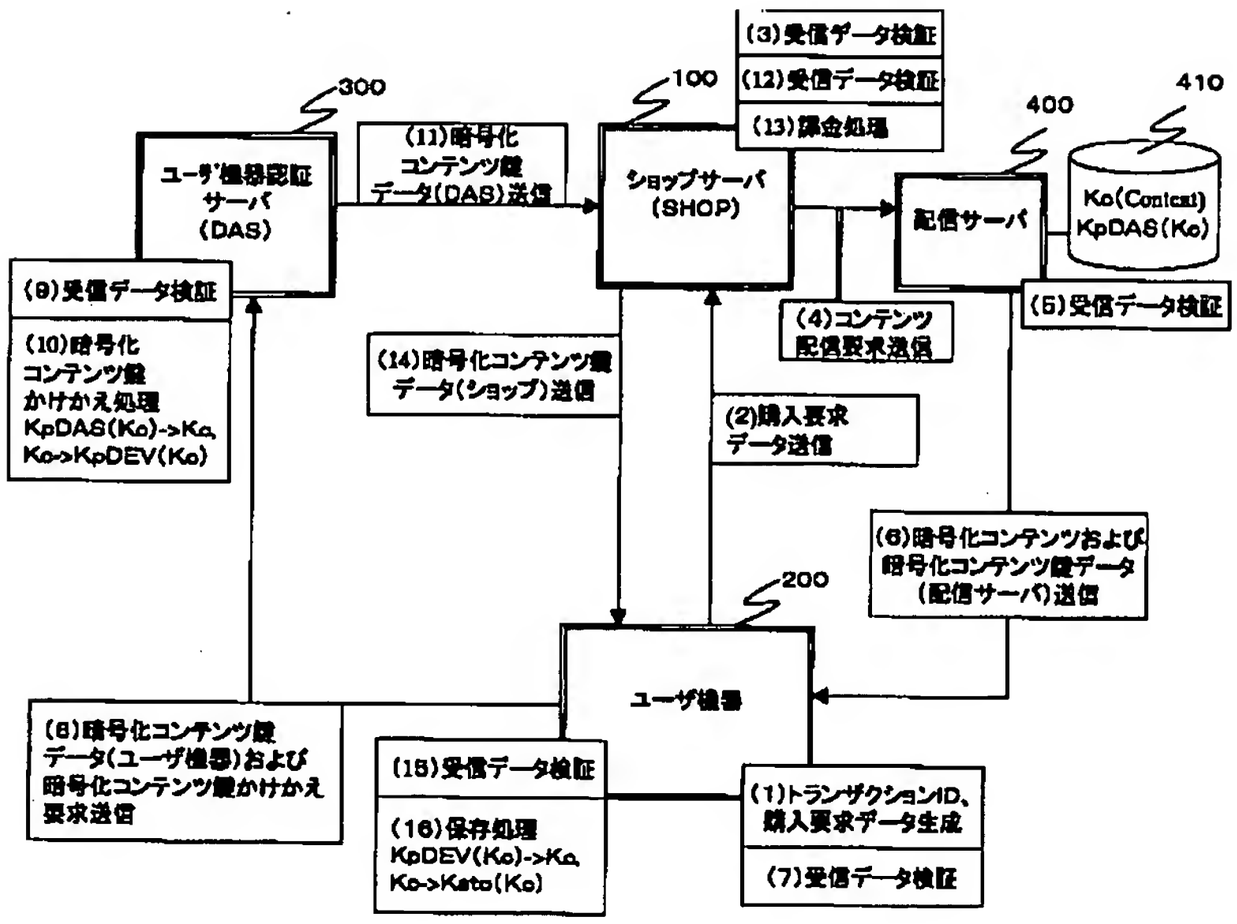


【図４０】

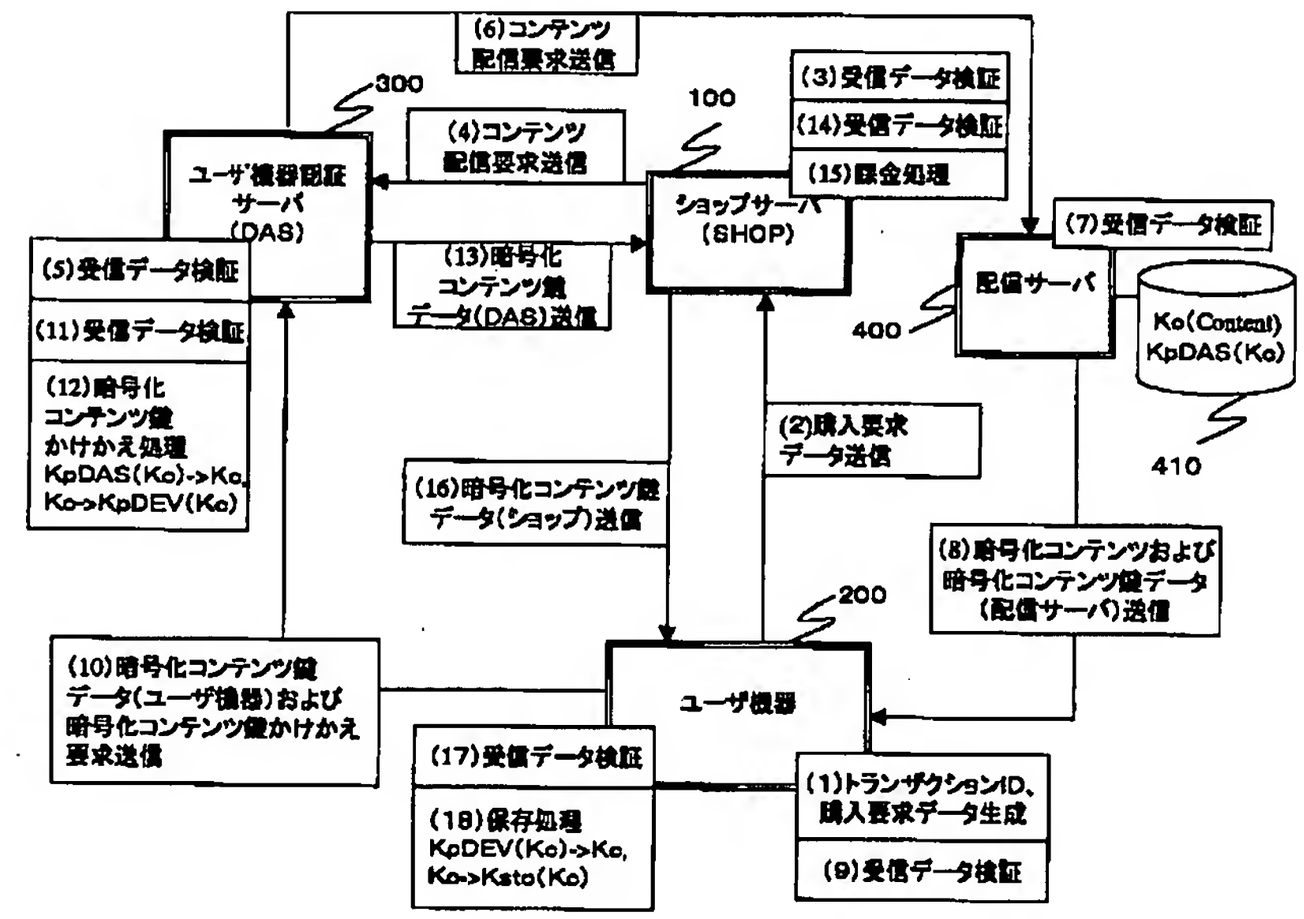
トランザクションID	コンテンツID	チケット発行体ID	チケット発行処理No.	チケット配信先ID	ステータス
999888777	5000	1234	10001	1234567890	鍵2受信完了
666555444	4050	1534	12345	2345678901	鍵1受信完了
999888779	5010	2351	15435	2233567890	電子チケット送信完了
333555444	4320	0989	10302	——	電子チケット受信完了
2133545445	3232	3549	22543	——	購入要求送信完了

ユーザ機器・購入管理DB

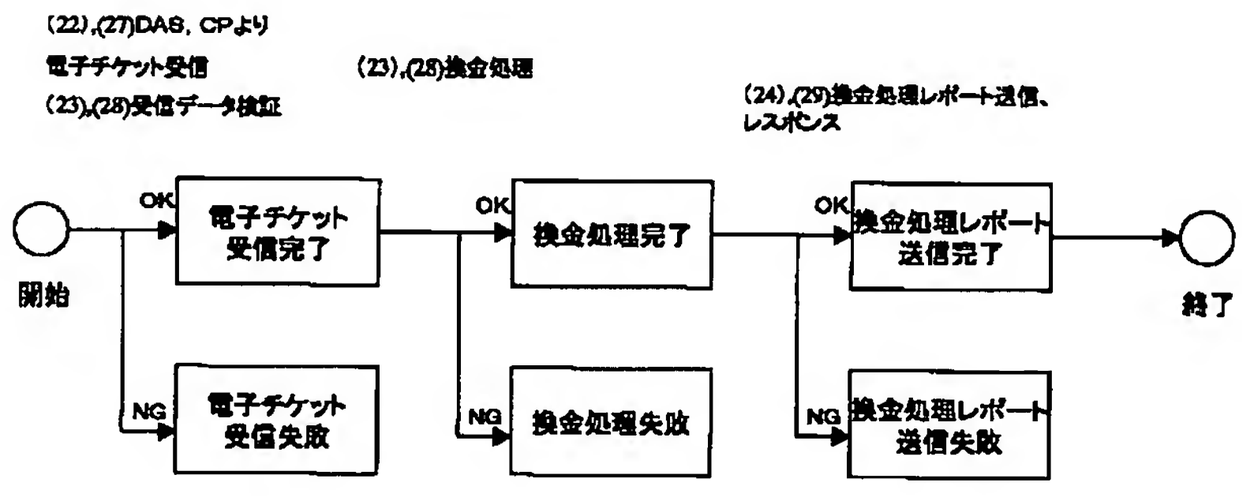
【図２９】


(3)受信データ検証
(12)受信データ検証
(13)課金処理
300
100
400
410
ユーザ機器認証
サーバ
(DAS)
(11)暗号化
コンテンツ鍵
データ(DAS)送信
ショップサーバ
(SHOP)
配信サーバ
Ko(Content)
KpDAS(Ko)
(9)受信データ検証
(10)暗号化
コンテンツ鍵
かけかえ処理
KpDAS(Ko)->Ko,
Ko->KpDEV(Ko)
(14)暗号化コンテンツ鍵
データ(ショップ)送信
(4)コンテンツ
配信要求送信
(5)受信データ検証
(2)購入要求
データ送信
(6)暗号化コンテンツおよび
暗号化コンテンツ鍵データ
(配信サーバ)送信
200
ユーザ機器
(8)暗号化コンテンツ鍵
データ(ユーザ機器)および
暗号化コンテンツ鍵かけかえ
要求送信
(15)受信データ検証
(16)保存処理
KpDEV(Ko)->Ko,
Ko->Ksto(Ko)
(1)トランザクションID、
購入要求データ生成
(7)受信データ検証

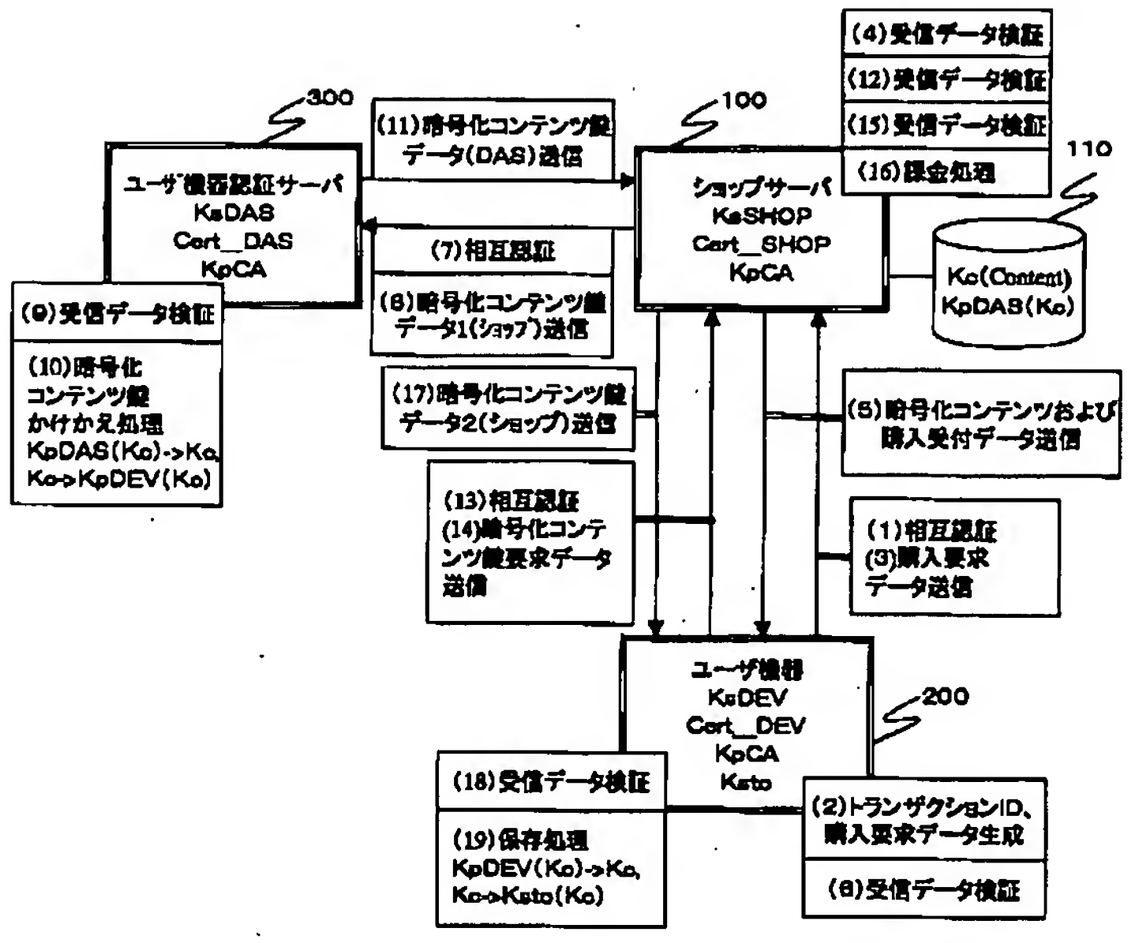
【図３０】


(6)コンテンツ
配信要求送信
300
100
(3)受信データ検証
(14)受信データ検証
(15)課金処理
ユーザ機器認証
サーバ
(DAS)
(4)コンテンツ
配信要求送信
ショップサーバ
(SHOP)
(7)受信データ検証
(5)受信データ検証
(13)暗号化
コンテンツ鍵
データ(DAS)送信
配信サーバ
400
Ko(Content)
KpDAS(Ko)
(11)受信データ検証
(12)暗号化
コンテンツ鍵
かけかえ処理
KpDAS(Ko)->Ko,
Ko->KpDEV(Ko)
(2)購入要求
データ送信
410
(16)暗号化コンテンツ鍵
データ(ショップ)送信
(8)暗号化コンテンツおよび
暗号化コンテンツ鍵データ
(配信サーバ)送信
200
(10)暗号化コンテンツ鍵
データ(ユーザ機器)および
暗号化コンテンツ鍵かけかえ
要求送信
ユーザ機器
(17)受信データ検証
(18)保存処理
KpDEV(Ko)->Ko,
Ko->Ksto(Ko)
(1)トランザクションID、
購入要求データ生成
(9)受信データ検証

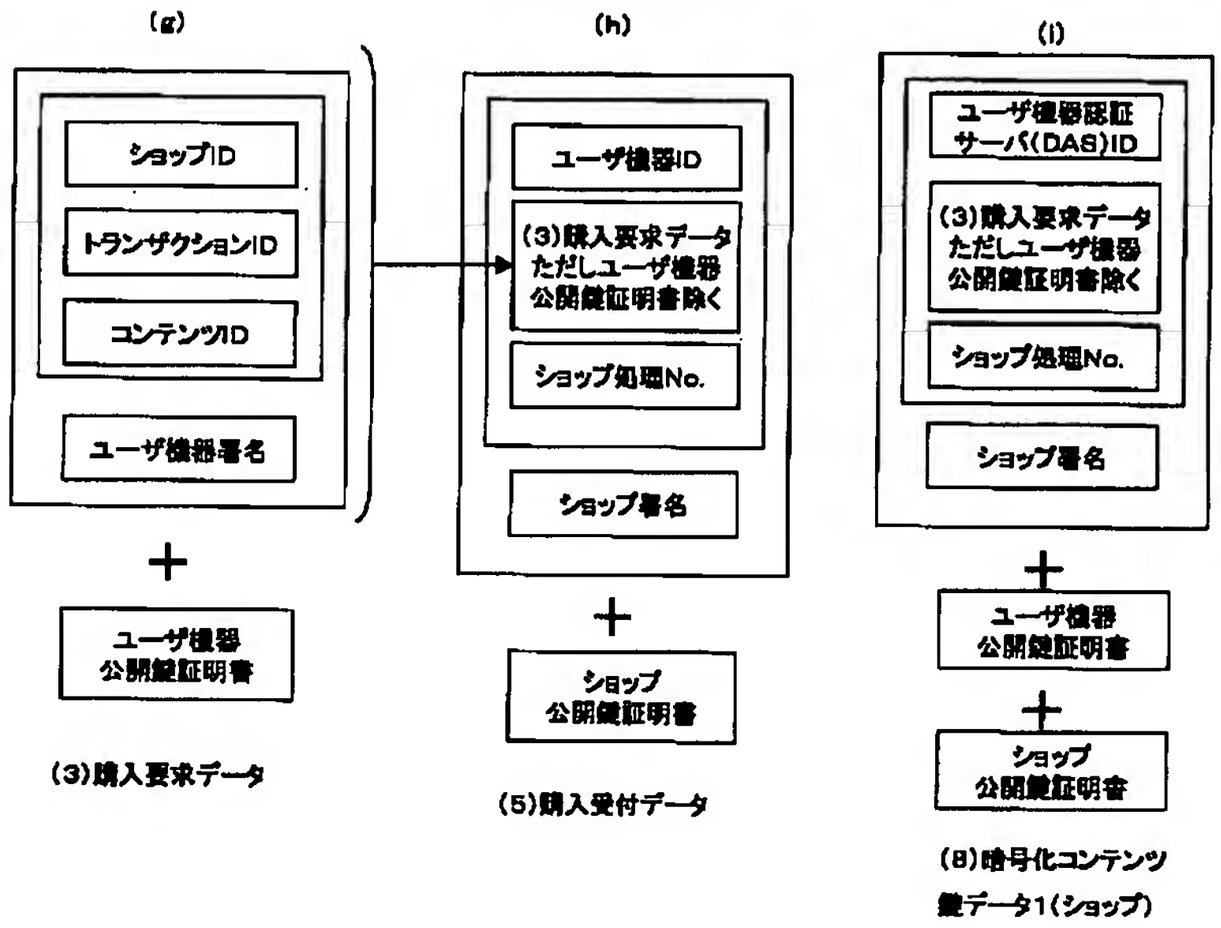
【図５２】


(22),(27)DAS, CPより
電子チケット受信
(23),(28)受信データ検証
(23),(28)換金処理
(24),(29)換金処理レポート送信、
レスポンス
開始
OK
電子チケット
受信完了
OK
換金処理完了
OK
換金処理レポート
送信完了
終了
NG
電子チケット
受信失敗
NG
換金処理失敗
NG
換金処理レポート
送信失敗

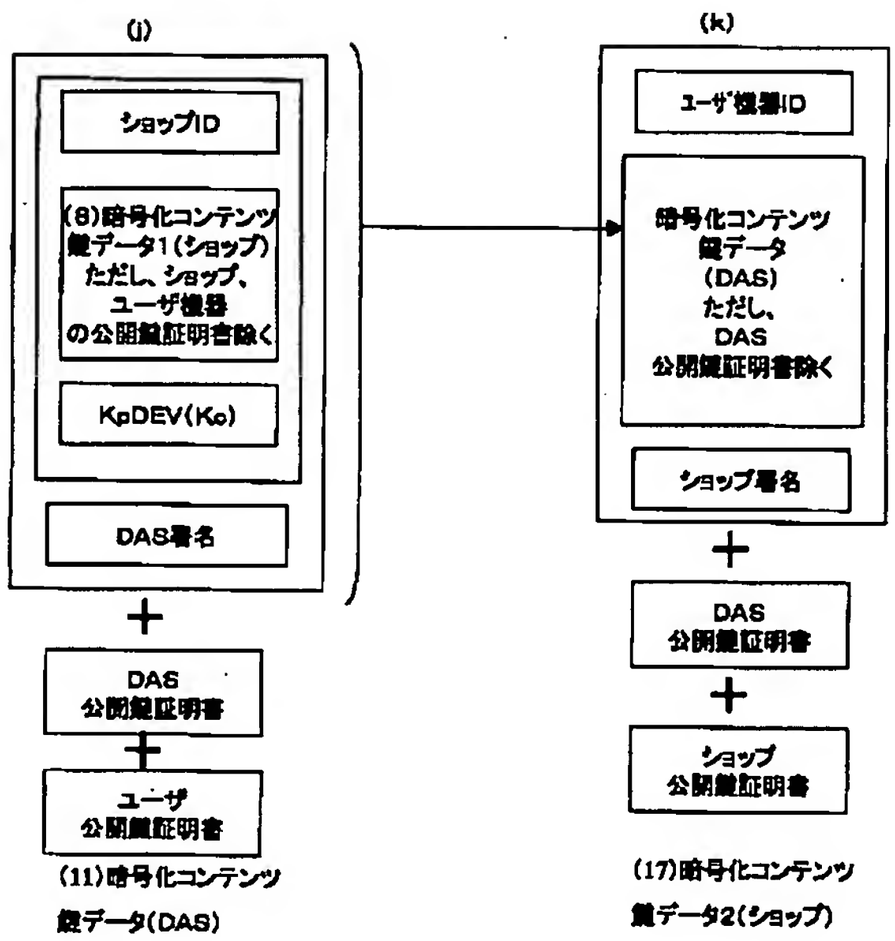
【図３１】


300
ユーザ機器認証サーバ
KsDAS
Cert_DAS
KpCA
(9)受信データ検証
(10)暗号化
コンテンツ鍵
かけかえ処理
KpDAS(Ko)->Ko,
Ko->KpDEV(Ko)
(11)暗号化コンテンツ鍵
データ(DAS)送信
(7)相互認証
(8)暗号化コンテンツ鍵
データ1(ショップ)送信
100
ショップサーバ
KsSHOP
Cert_SHOP
KpCA
(4)受信データ検証
(12)受信データ検証
(15)受信データ検証
(16)課金処理
110
Ko(Content)
KpDAS(Ko)
(17)暗号化コンテンツ鍵
データ2(ショップ)送信
(5)暗号化コンテンツおよび
購入受付データ送信
(13)相互認証
(14)暗号化コンテン
ツ鍵要求データ
送信
(1)相互認証
(3)購入要求
データ送信
ユーザ機器
KsDEV
Cert_DEV
KpCA
Ksto
200
(18)受信データ検証
(19)保存処理
KpDEV(Ko)->Ko,
Ko->Ksto(Ko)
(2)トランザクションID、
購入要求データ生成
(6)受信データ検証

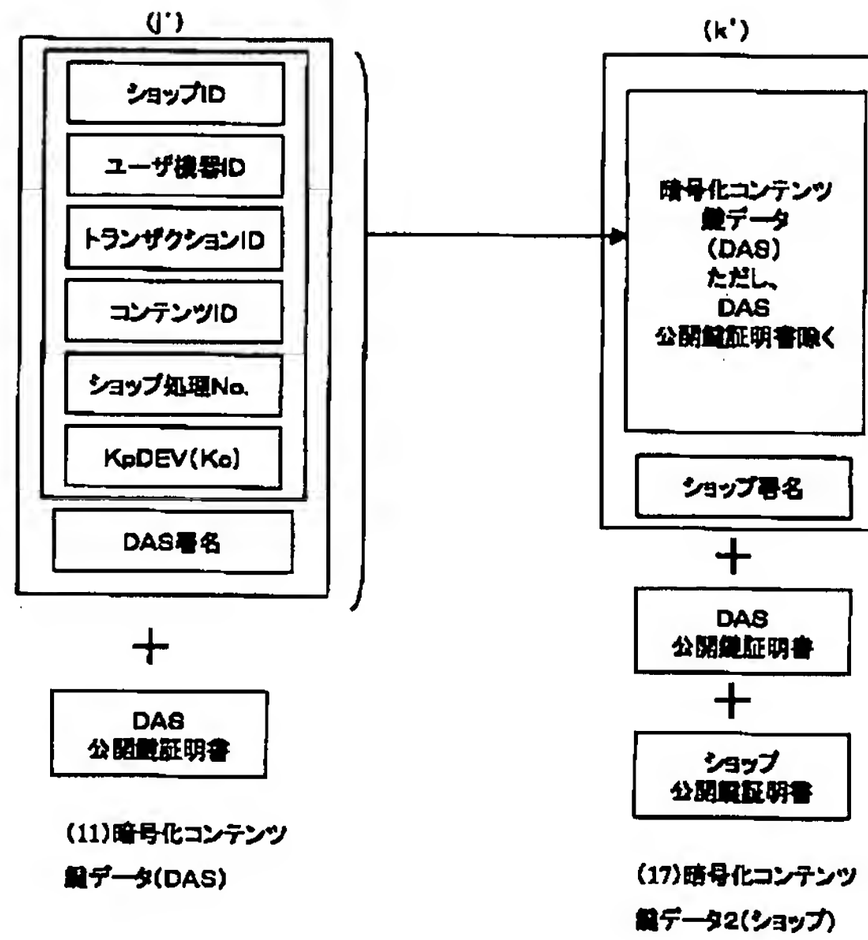
【図３２】


(g)
ショップID
トランザクションID
コンテンツID
ユーザ機器署名
ユーザ機器
公開鍵証明書
(3)購入要求データ
(h)
ユーザ機器ID
(3)購入要求データ
ただしユーザ機器
公開鍵証明書除く
ショップ処理No.
ショップ署名
ショップ
公開鍵証明書
(5)購入受付データ
(i)
ユーザ機器認証
サーバ(DAS)ID
(3)購入要求データ
ただしユーザ機器
公開鍵証明書除く
ショップ処理No.
ショップ署名
ユーザ機器
公開鍵証明書
ショップ
公開鍵証明書
(8)暗号化コンテンツ
鍵データ1(ショップ)

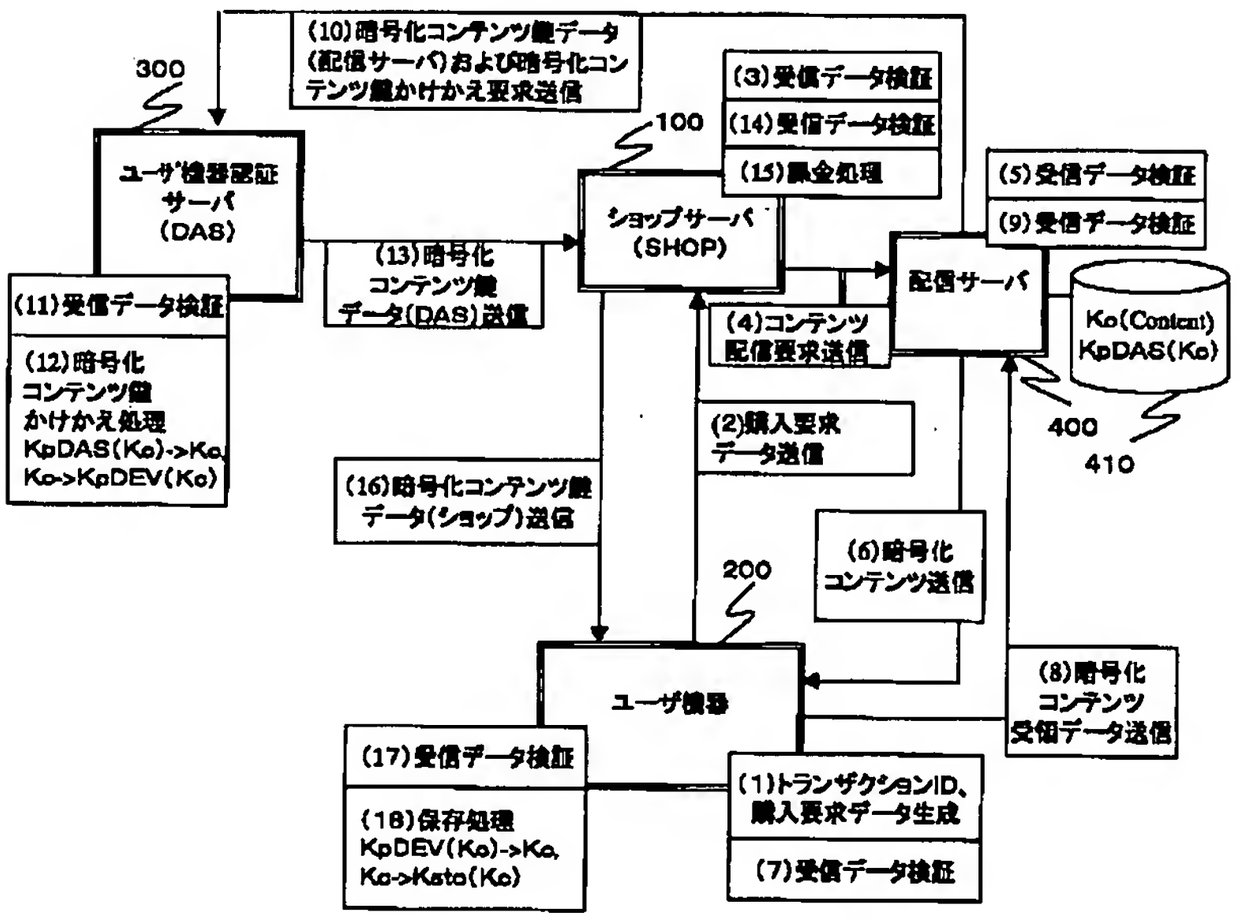
【図３３】



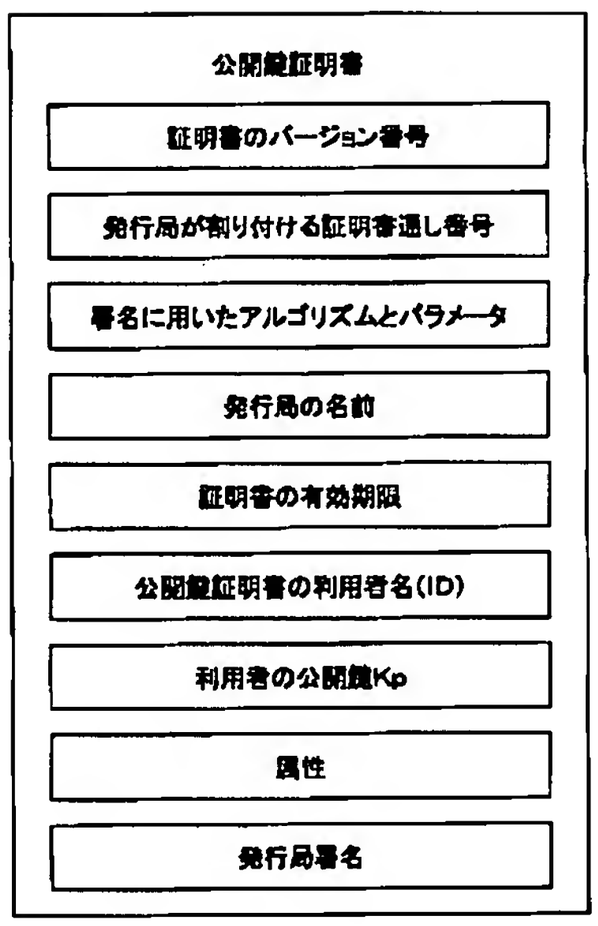
【図３４】



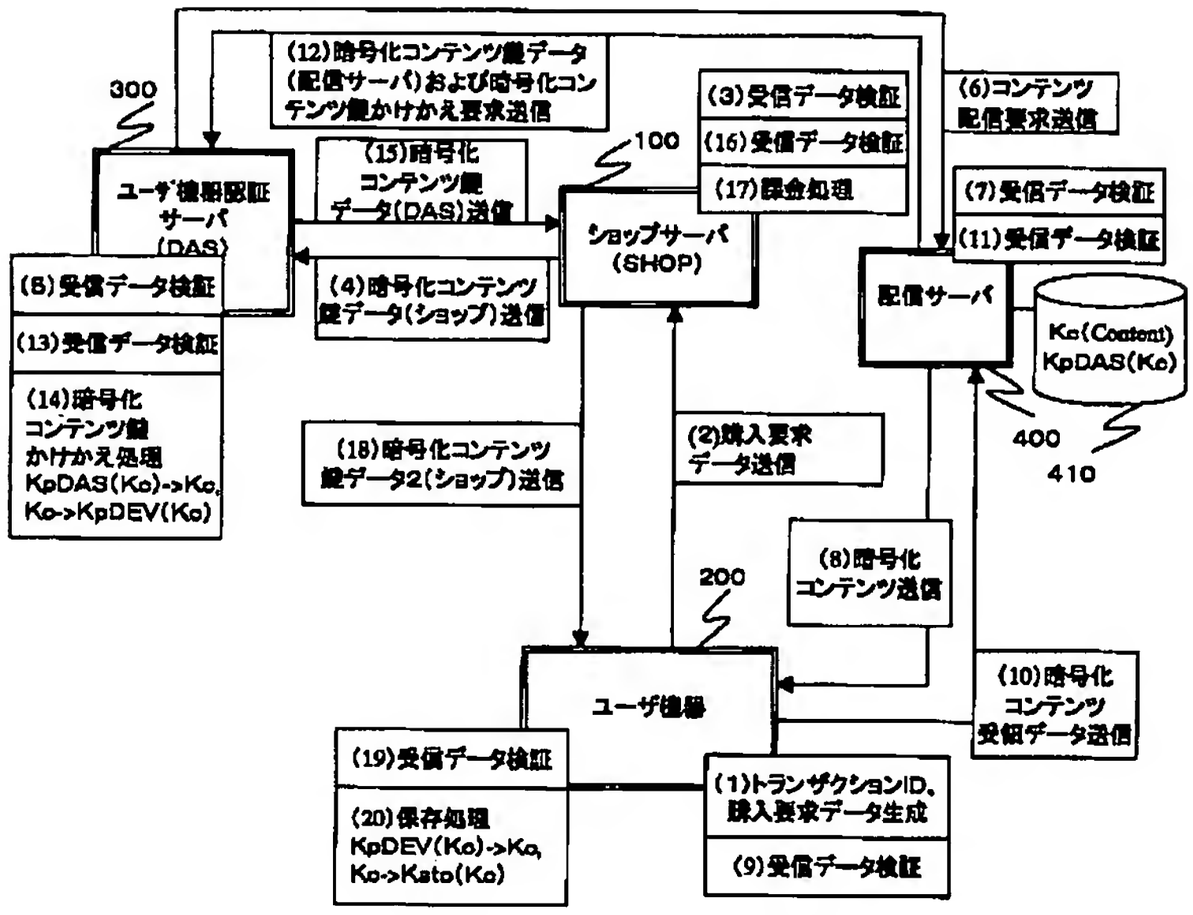
【図３５】



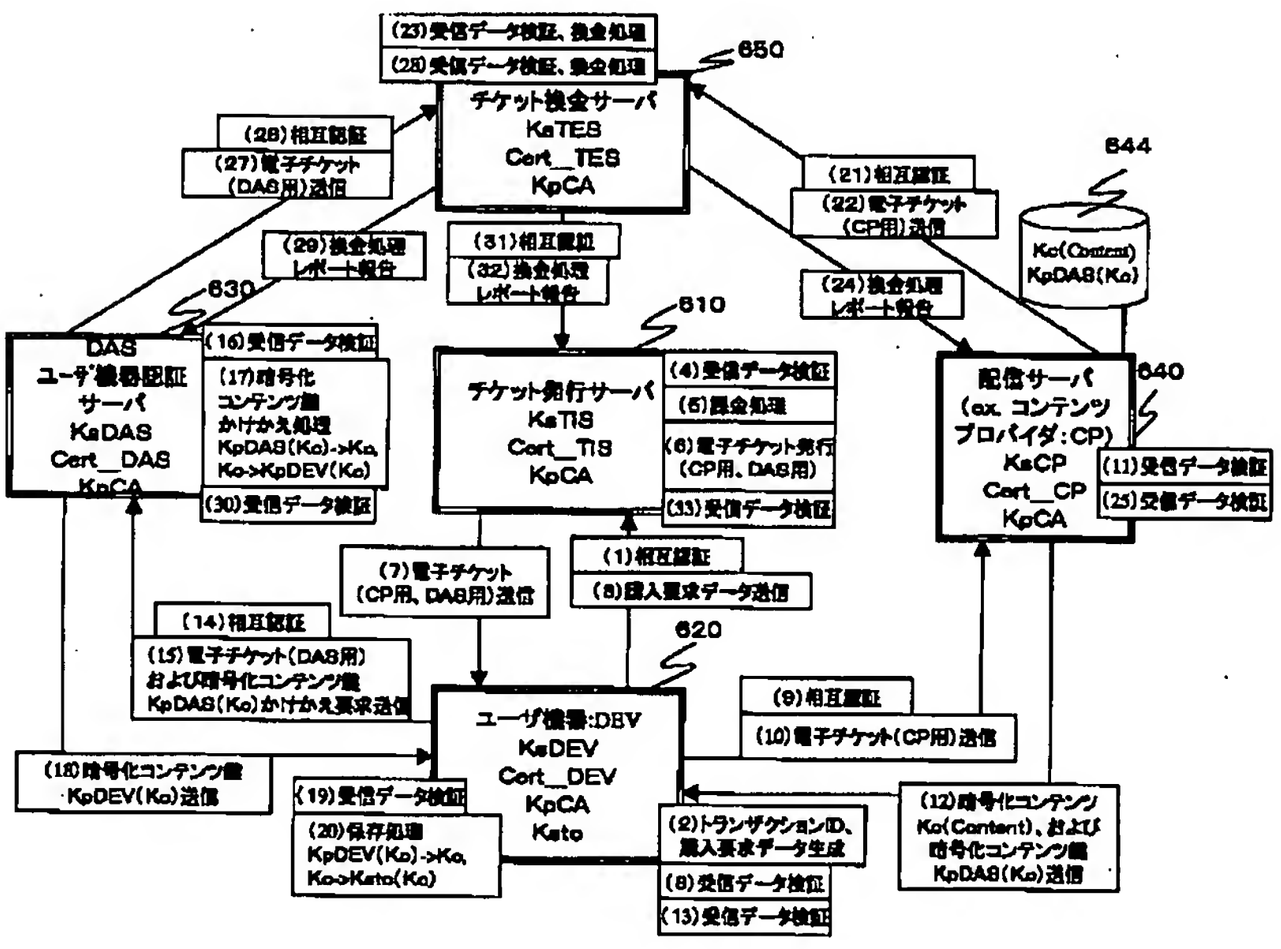
【図６７】



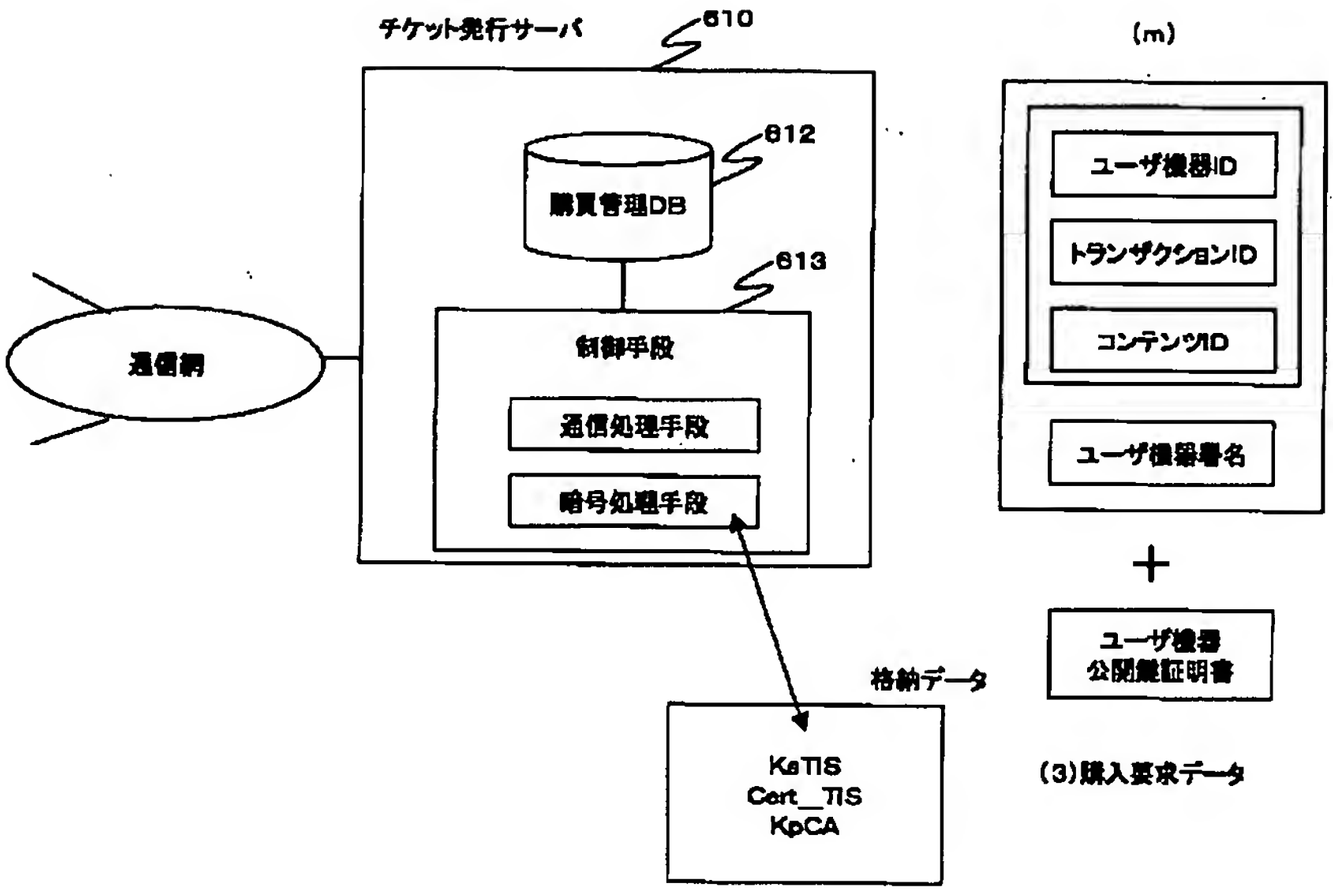
【図３６】


(12)暗号化コンテンツ鍵データ(配信サーバ)および暗号化コンテンツ鍵かけかえ要求送信
300
(3)受信データ検証
(16)受信データ検証
(17)課金処理
100
(6)コンテンツ配信要求送信
(15)暗号化コンテンツ鍵データ(DAS)送信
ユーザ機器認証サーバ(DAS)
ショップサーバ(SHOP)
(7)受信データ検証
(11)受信データ検証
(5)受信データ検証
(13)受信データ検証
(14)暗号化コンテンツ鍵かけかえ処理 KpDAS(Ko)->Ko, Ko->KpDEV(Ko)
(4)暗号化コンテンツ鍵データ(ショップ)送信
配信サーバ
Ko(Content) KpDAS(Ko)
400
410
(18)暗号化コンテンツ鍵データ2(ショップ)送信
(2)購入要求データ送信
(8)暗号化コンテンツ送信
200
ユーザ機器
(10)暗号化コンテンツ受信データ送信
(19)受信データ検証
(20)保存処理 KpDEV(Ko)->Ko, Ko->Kato(Ko)
(1)トランザクションID、購入要求データ生成
(9)受信データ検証

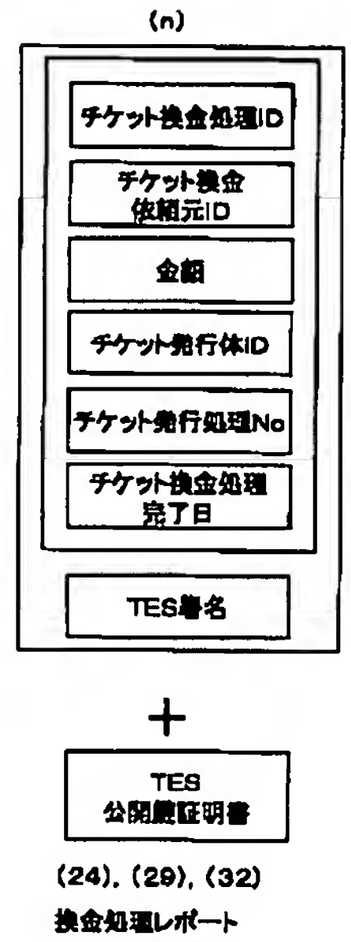
【図３７】


(23)受信データ検証、課金処理
(26)受信データ検証、課金処理
650
チケット課金サーバ KsTES Cert_TES KpCA
(28)相互認証
(27)電子チケット(DAS用)送信
(21)相互認証
(22)電子チケット(CP用)送信
644
Ko(Content) KpDAS(Ko)
(29)課金処理レポート報告
(31)相互認証
(32)課金処理レポート報告
(24)課金処理レポート報告
630
610
640
DAS ユーザ機器認証サーバ KsDAS Cert_DAS KpCA
(16)受信データ検証
(17)暗号化コンテンツ鍵かけかえ処理 KpDAS(Ko)->Ko, Ko->KpDEV(Ko)
(30)受信データ検証
チケット発行サーバ KsTIS Cert_TIS KpCA
(4)受信データ検証
(5)課金処理
(6)電子チケット発行(CP用、DAS用)
(33)受信データ検証
配信サーバ (ex. コンテンツプロバイダ:CP) KsCP Cert_CP KpCA
(11)受信データ検証
(25)受信データ検証
(7)電子チケット(CP用、DAS用)送信
(1)相互認証
(8)購入要求データ送信
(14)相互認証
(15)電子チケット(DAS用)および暗号化コンテンツ鍵 KpDAS(Ko)かけかえ要求送信
620
ユーザ機器:DEV KsDEV Cert_DEV KpCA Kato
(9)相互認証
(10)電子チケット(CP用)送信
(18)暗号化コンテンツ鍵 KpDEV(Ko)送信
(19)受信データ検証
(20)保存処理 KpDEV(Ko)->Ko, Ko->Kato(Ko)
(2)トランザクションID、購入要求データ生成
(12)暗号化コンテンツ Ko(Content)、および暗号化コンテンツ鍵 KpDAS(Ko)送信
(8)受信データ検証
(13)受信データ検証

【図３８】



【図４６】

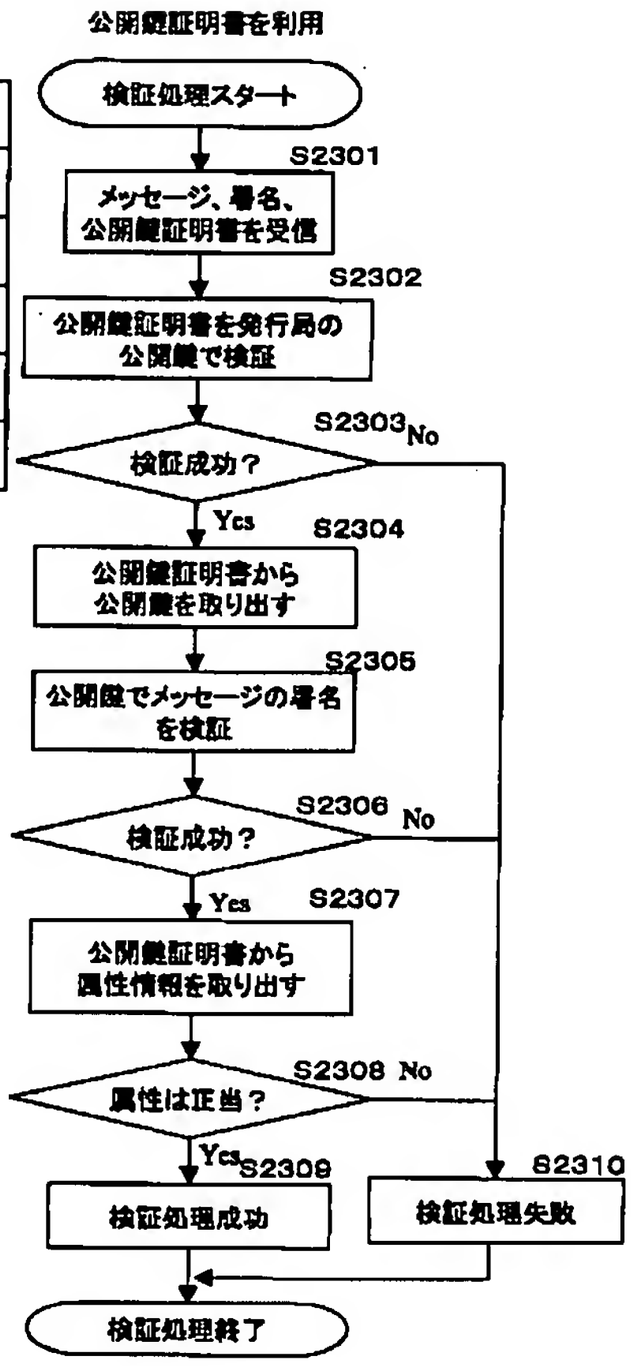


【図４１】

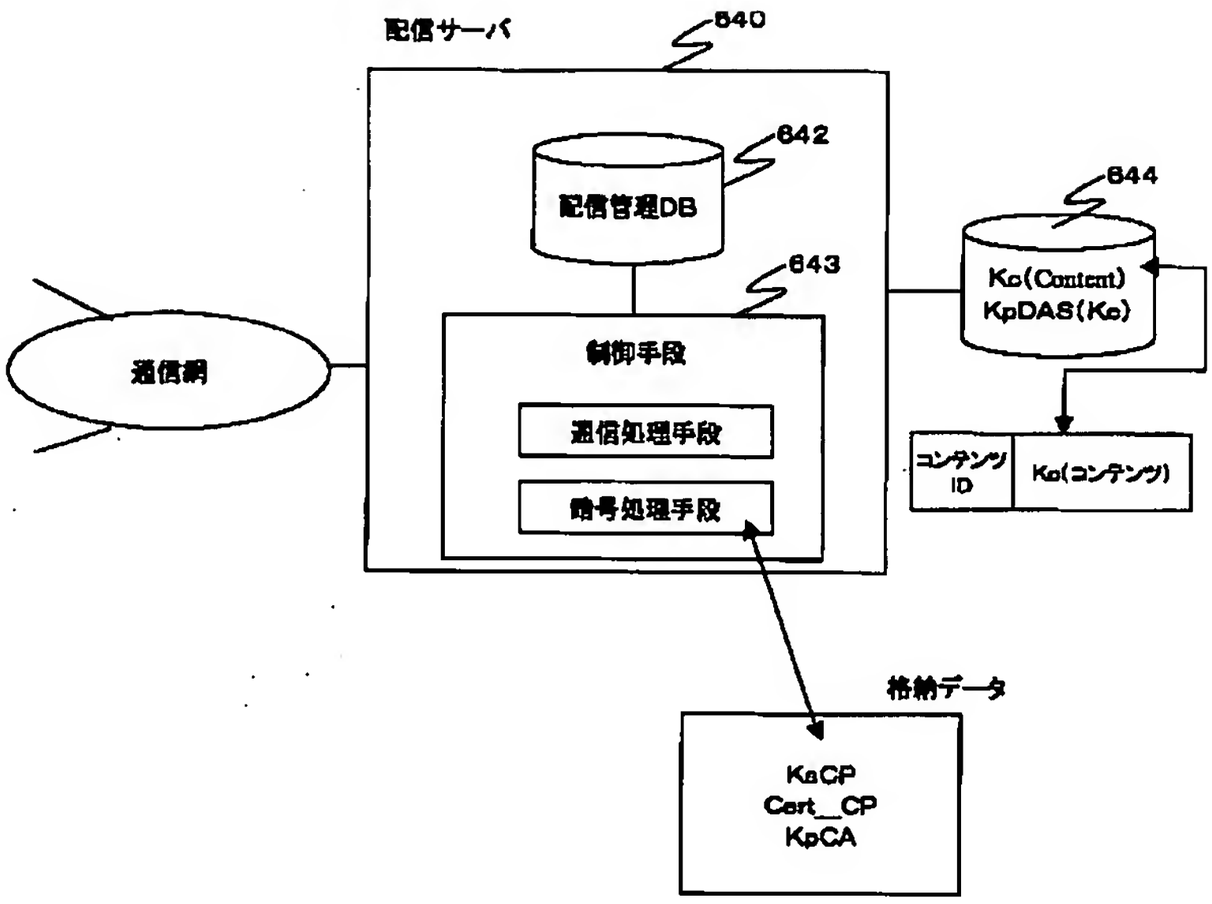
ユーザ機器認証サーバ処理No.	機器ID	トランザクションID	コンテンツID	チケット発行体ID	チケット発行処理No.	ステータス
50001	1234567890	999888777	5000	331234	10001	換金処理レポート受信完了
50002	2345678901	666555444	7050	345634	10025	チケット換金要求送信完了
50003	3456788901	321655444	8021	645234	10200	鍵送信完了
50004	5567778902	123555444	3245	321632	10325	鍵かけかえ完了
50005	5435678445	335655321	2651	764545	12300	鍵受信完了

ユーザ機器認証サーバ・ライセンス管理DB

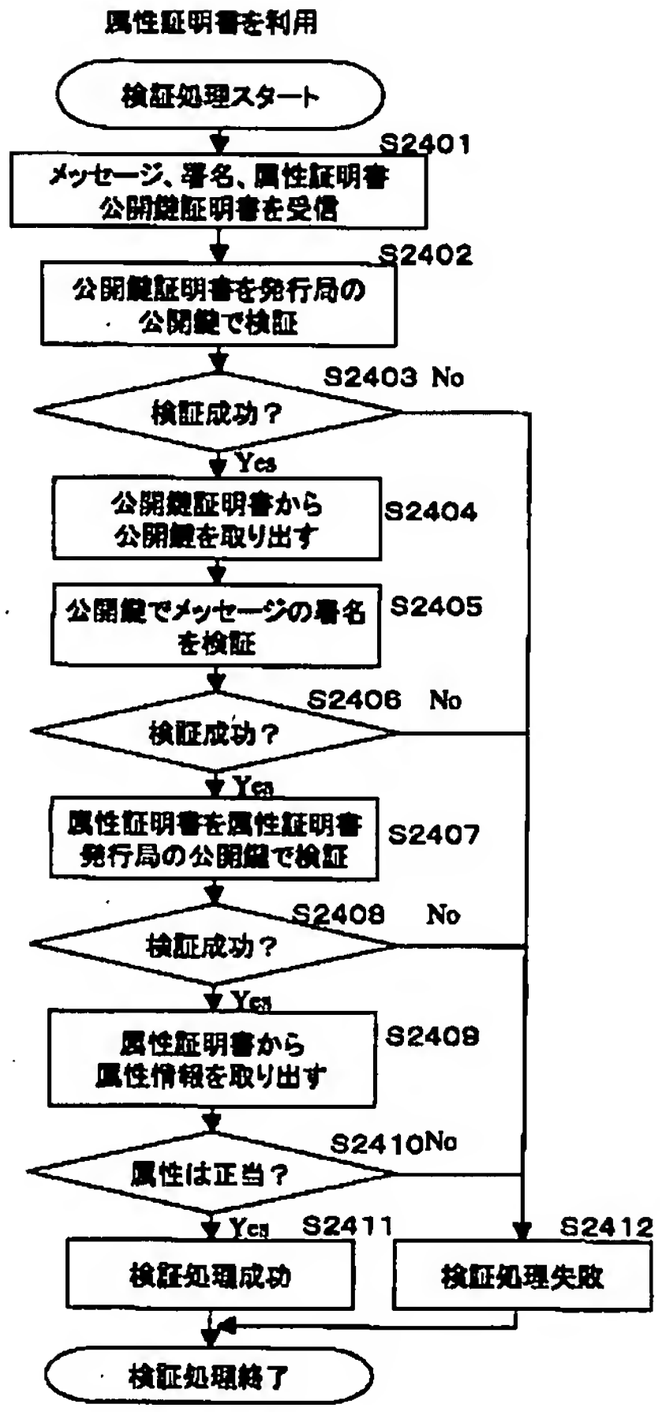
【図７５】



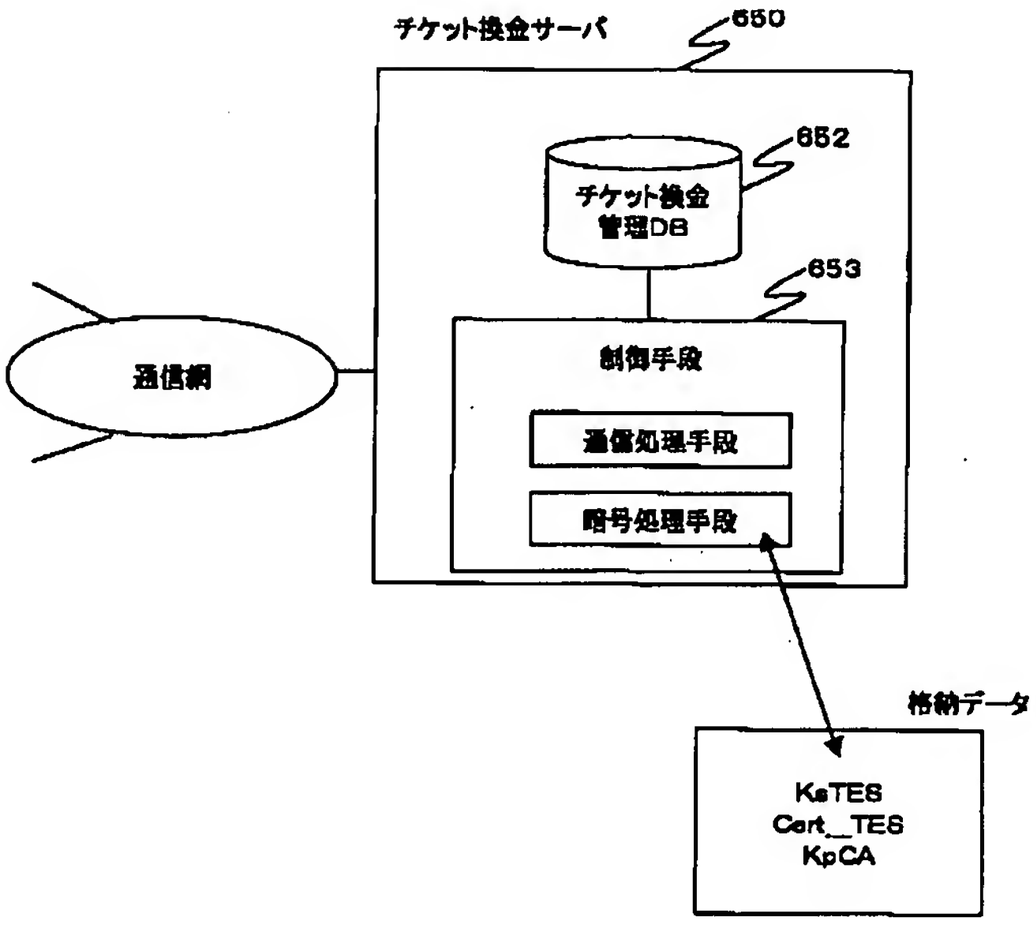
【図４２】


配信サーバ
640
642
配信管理DB
643
制御手段
通信処理手段
暗号処理手段
通信網
644
Kc(Content)
KpDAS(Kc)
コンテンツID
Kc(コンテンツ)
格納データ
KaCP
Cert_CP
KpCA

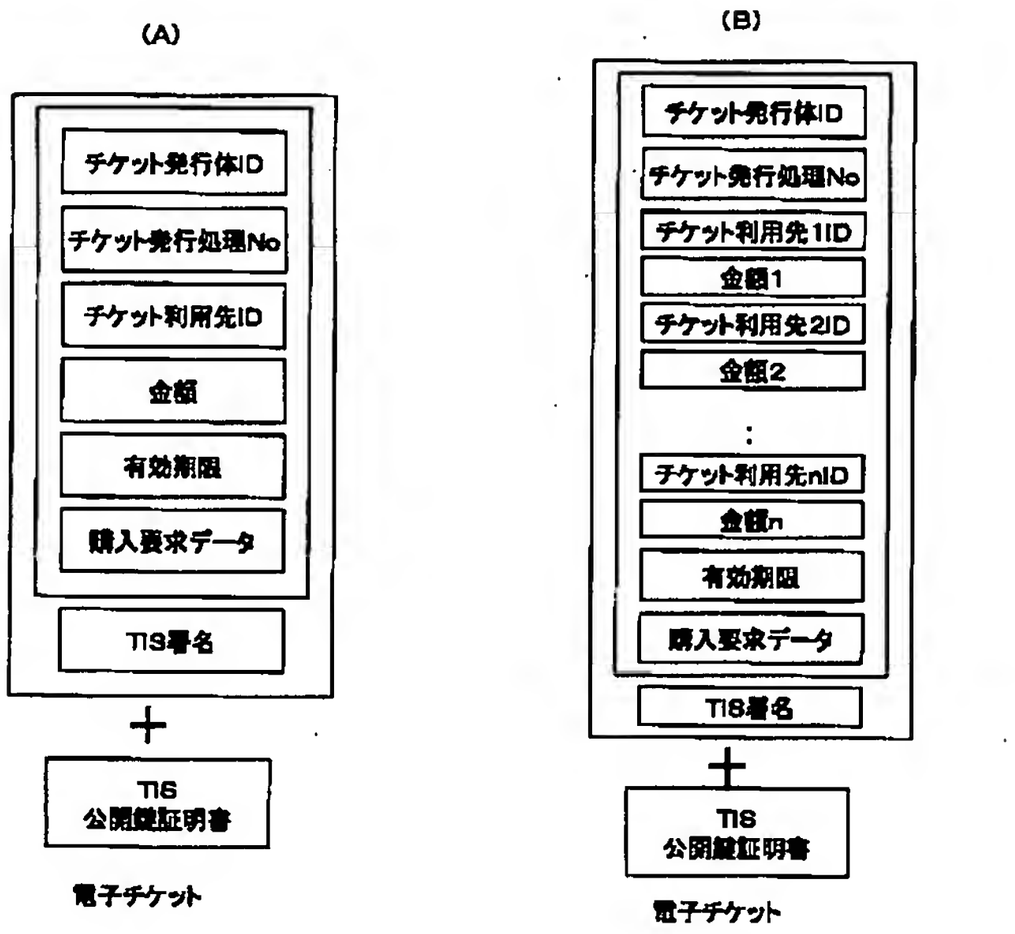
【図７６】


属性証明書を利用
検証処理スタート
S2401
メッセージ、署名、属性証明書
公開鍵証明書を受信
S2402
公開鍵証明書を発行局の
公開鍵で検証
S2403 No
検証成功？
Yes
公開鍵証明書から
公開鍵を取り出す
S2404
公開鍵でメッセージの署名
を検証
S2405
S2406 No
検証成功？
Yes
属性証明書を属性証明書
発行局の公開鍵で検証
S2407
S2408 No
検証成功？
Yes
属性証明書から
属性情報を取り出す
S2409
S2410No
属性は正当？
Yes
S2411
S2412
検証処理成功
検証処理失敗
検証処理終了

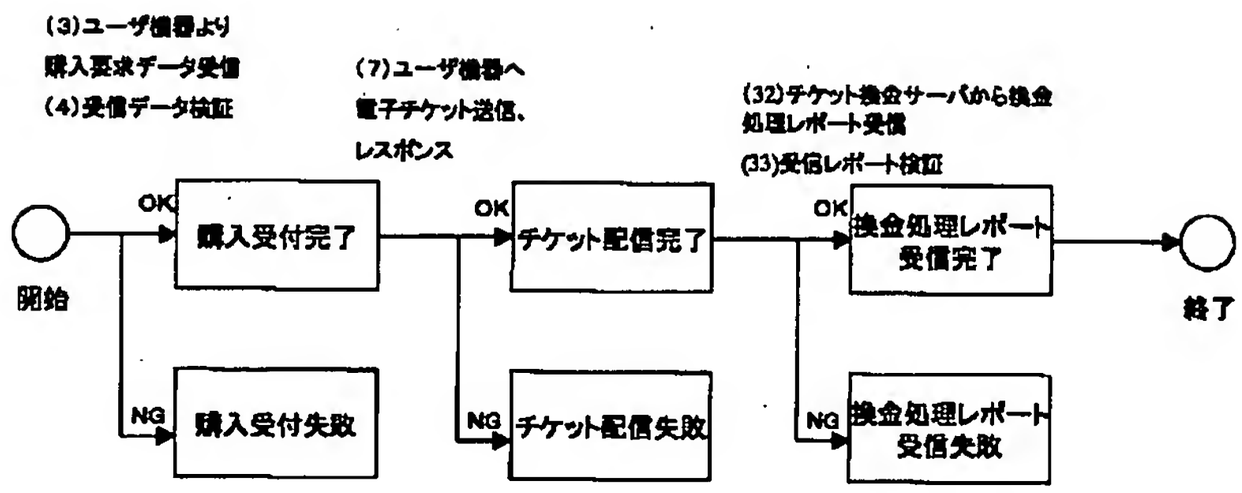
【図４４】


チケット換金サーバ
650
652
チケット換金
管理DB
653
制御手段
通信処理手段
暗号処理手段
通信網
格納データ
KaTES
Cert_TES
KpCA

【図４７】



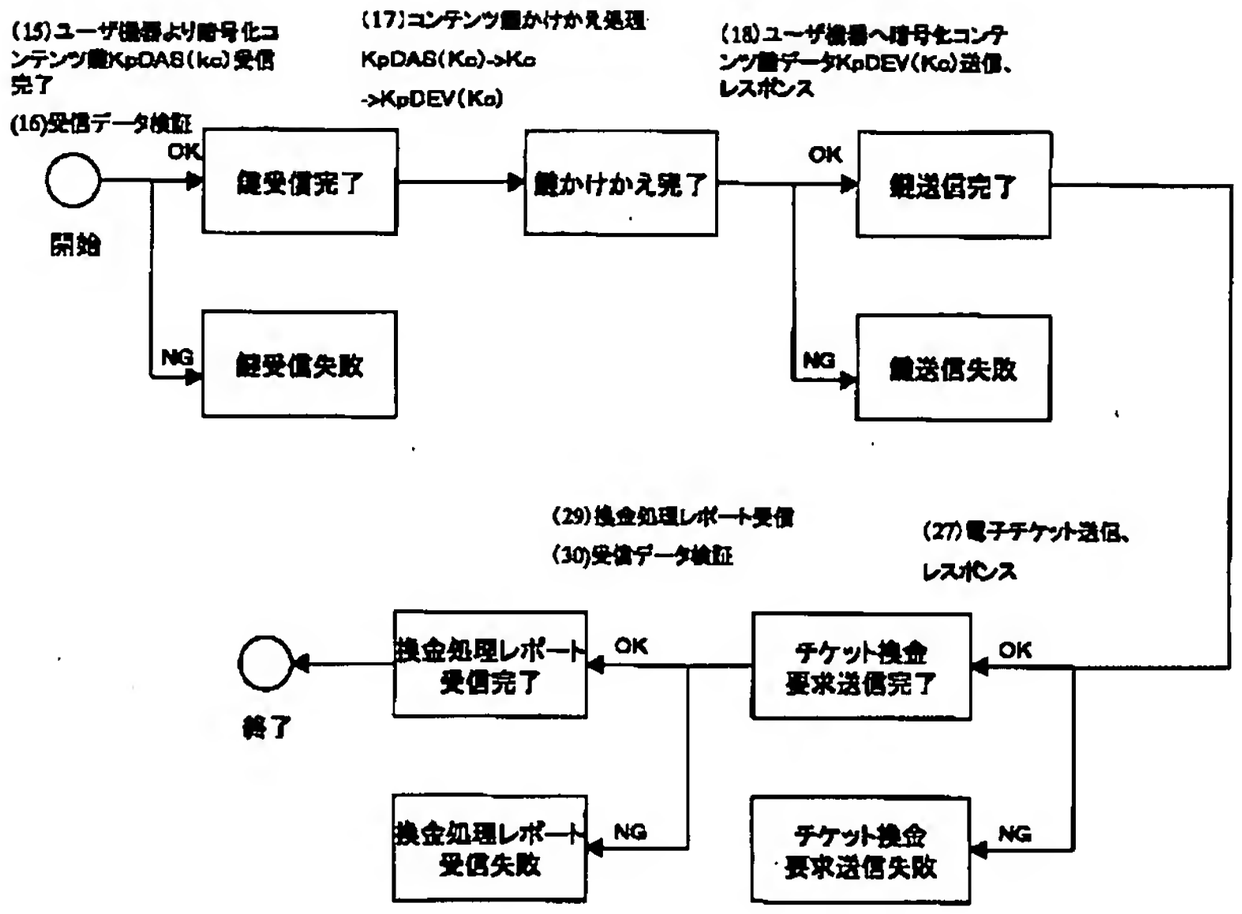
【図４８】



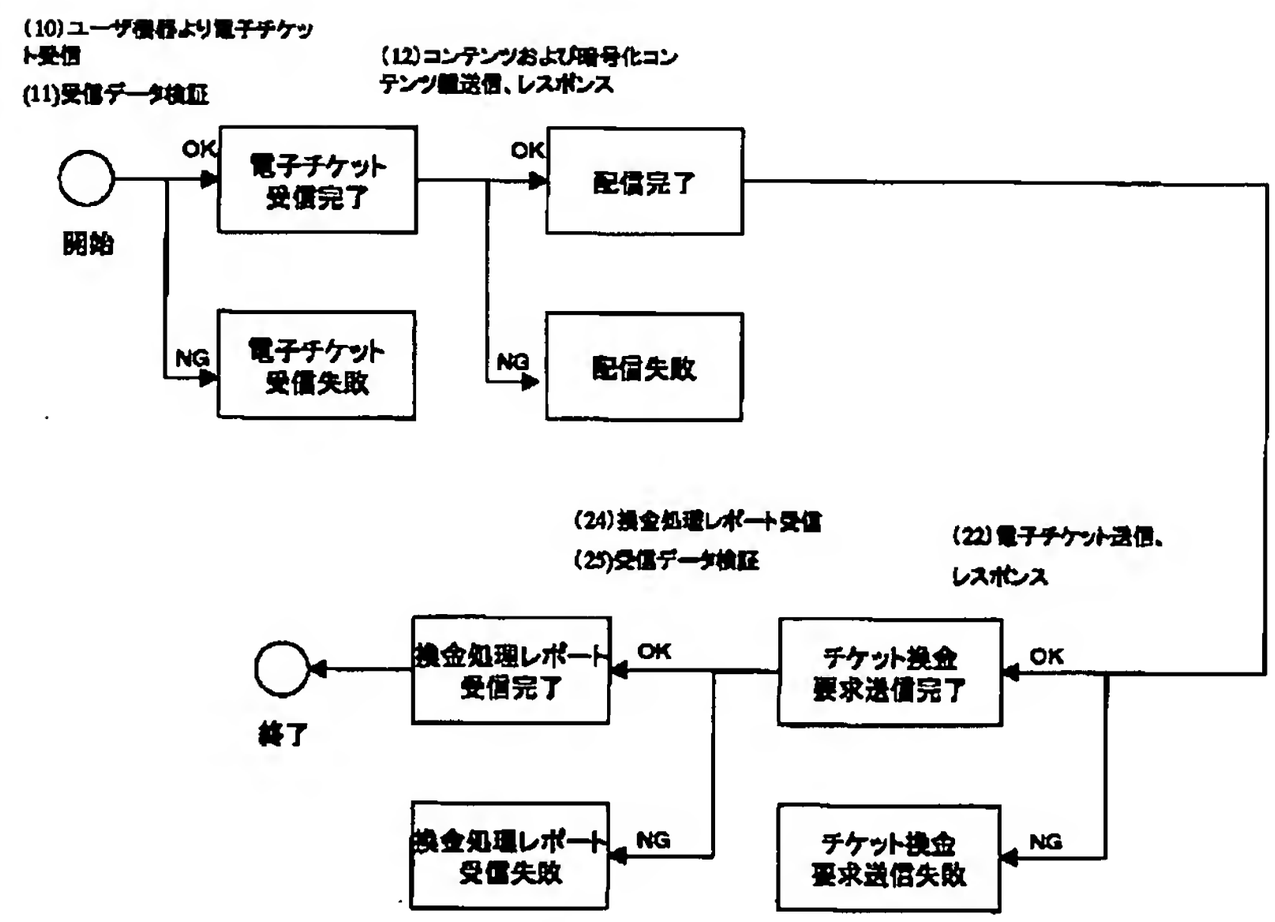
【図６６】

属性コード(2バイト)	エンティティ	機能
0000	登録局(RA)	公開鍵証明書、属性証明書の発行審査を行なう
0001	サービス運営者(SH)	システム上で流通するコンテンツのライセンス料を徴収する ex. コンテンツを復号するタメの鍵のかけ替え処理、ログ情報の収集
0002	コンテンツ販売者(SHOP)	ユーザにコンテンツ内容を提示し、コンテンツ販売代金を徴収する
0003	コンテンツ配信者	コンテンツ販売者の要求に応じ、ユーザにコンテンツを配信する
0004	ユーザ機器	コンテンツの購入、利用を行なう
:	:	:

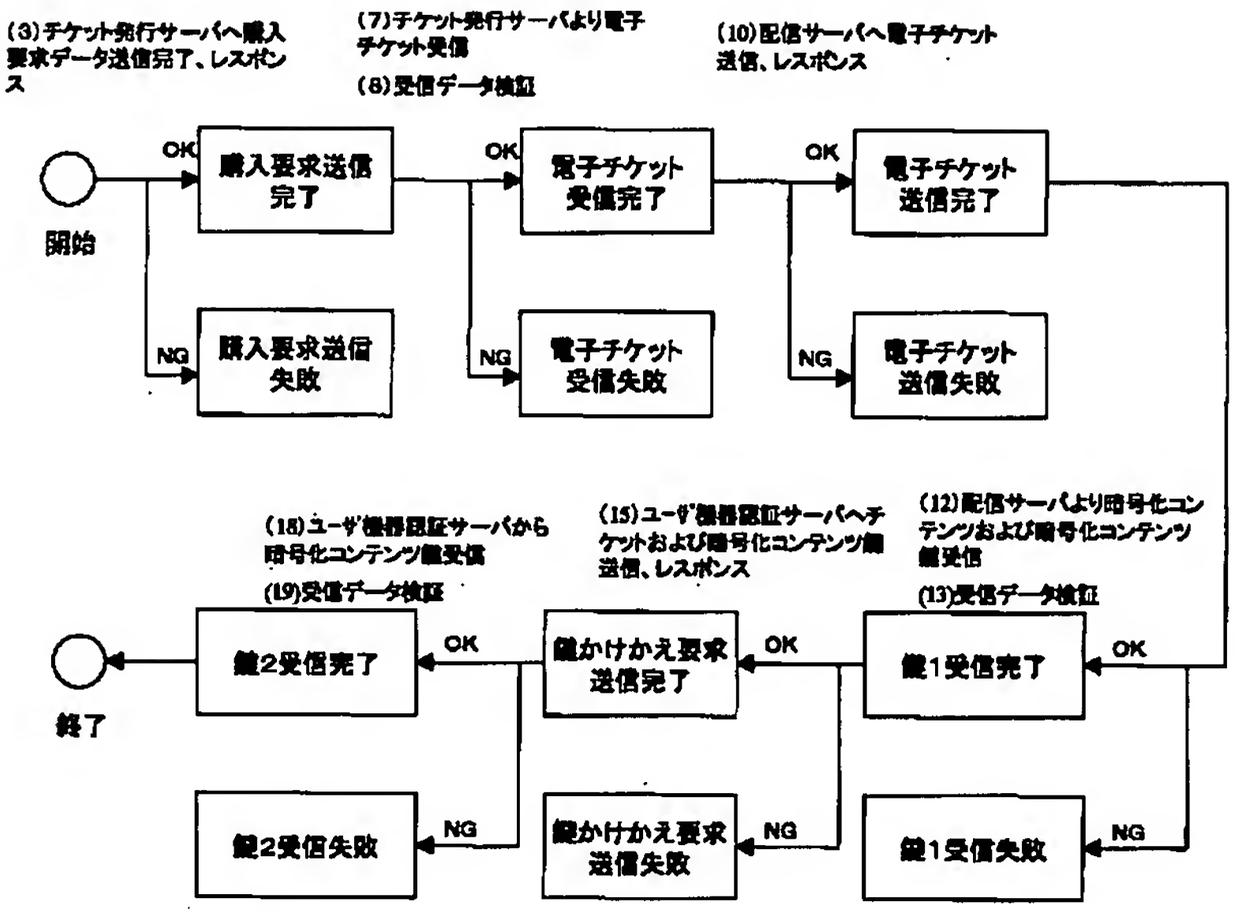
【図４９】


(15)ユーザ機器より暗号化コンテンツ鍵KpDAS(kc)受信完了
(16)受信データ検証
(17)コンテンツ鍵かけかえ処理
KpDAS(Kc)->Kc
->KpDEV(Kc)
(18)ユーザ機器へ暗号化コンテンツ鍵データKpDEV(Kc)送信、レスポンス
OK
鍵受信完了
鍵かけかえ完了
OK
鍵送信完了
開始
NG
鍵受信失敗
NG
鍵送信失敗
(29)換金処理レポート受信
(30)受信データ検証
(27)電子チケット送信、レスポンス
換金処理レポート受信完了
OK
チケット換金要求送信完了
OK
終了
換金処理レポート受信失敗
NG
チケット換金要求送信失敗
NG

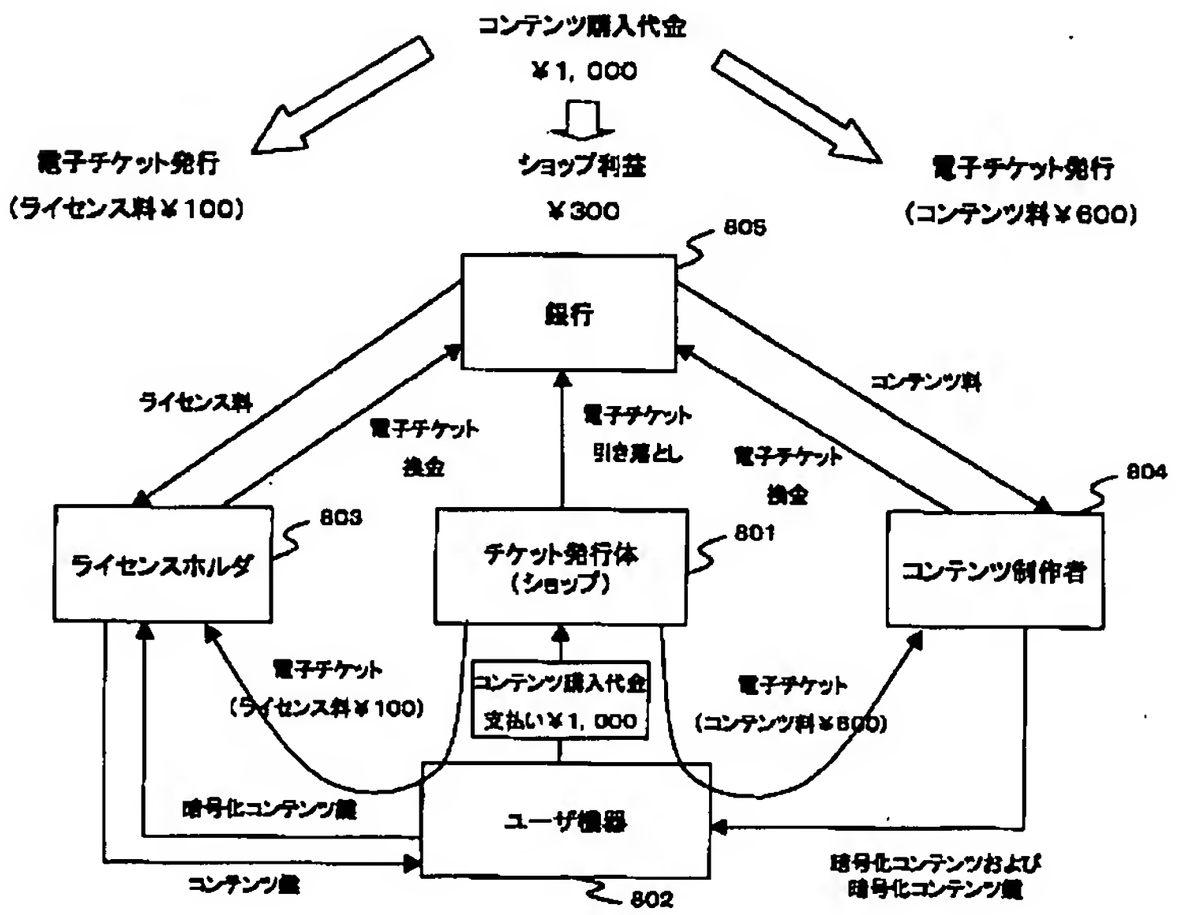
【図５０】


(10)ユーザ機器より電子チケット受信
(11)受信データ検証
(12)コンテンツおよび暗号化コンテンツ鍵送信、レスポンス
OK
電子チケット受信完了
OK
配信完了
開始
NG
電子チケット受信失敗
NG
配信失敗
(24)換金処理レポート受信
(25)受信データ検証
(22)電子チケット送信、レスポンス
換金処理レポート受信完了
OK
チケット換金要求送信完了
OK
終了
換金処理レポート受信失敗
NG
チケット換金要求送信失敗
NG

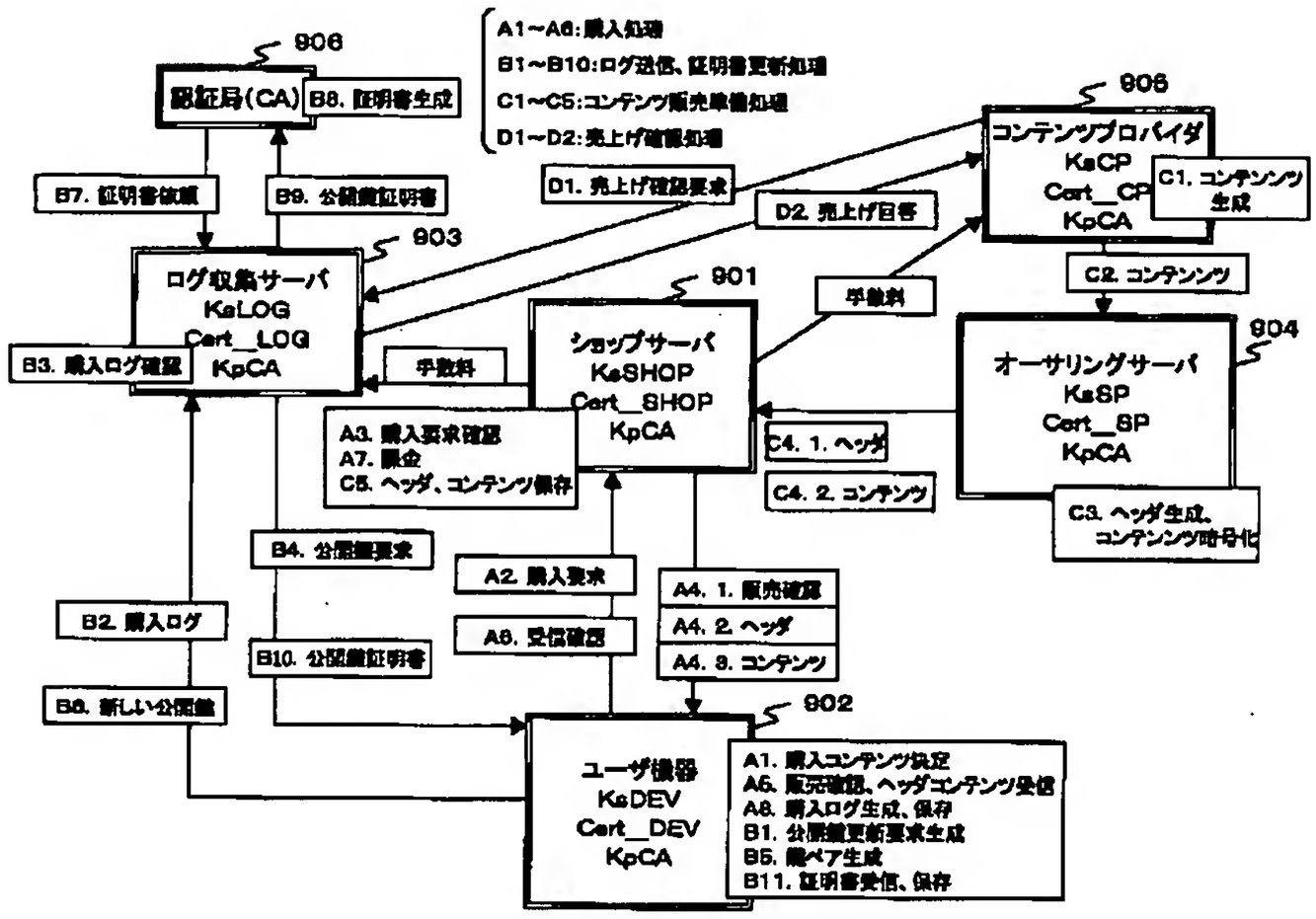
【図５１】


(3)チケット発行サーバへ購入要求データ送信完了、レスポンス
(7)チケット発行サーバより電子チケット受信
(8)受信データ検証
(10)配信サーバへ電子チケット送信、レスポンス
開始
OK
購入要求送信完了
NG
購入要求送信失敗
OK
電子チケット受信完了
NG
電子チケット受信失敗
OK
電子チケット送信完了
NG
電子チケット送信失敗
(18)ユーザ機器認証サーバから暗号化コンテンツ鍵受信
(19)受信データ検証
(15)ユーザ機器認証サーバへチケットおよび暗号化コンテンツ鍵送信、レスポンス
(12)配信サーバより暗号化コンテンツおよび暗号化コンテンツ鍵受信
(13)受信データ検証
終了
鍵2受信完了
OK
鍵2受信失敗
NG
鍵かけかえ要求送信完了
OK
鍵かけかえ要求送信失敗
NG
鍵1受信完了
OK
鍵1受信失敗
NG

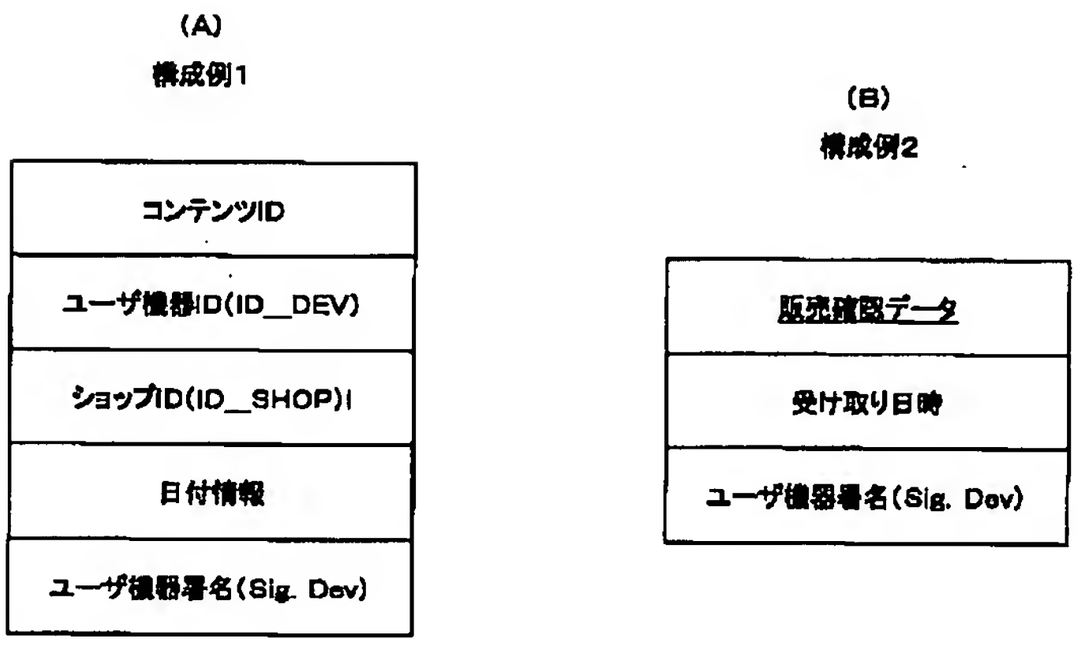
【図５３】


コンテンツ購入代金
￥1，000
電子チケット発行
（ライセンス料￥100）
ショップ利益
￥300
電子チケット発行
（コンテンツ料￥600）
805
銀行
ライセンス料
電子チケット
換金
電子チケット
引き落とし
電子チケット
換金
コンテンツ料
804
803
ライセンスホルダ
801
チケット発行体
（ショップ）
コンテンツ制作者
電子チケット
（ライセンス料￥100）
コンテンツ購入代金
支払い￥1，000
電子チケット
（コンテンツ料￥600）
暗号化コンテンツ鍵
ユーザ機器
コンテンツ鍵
暗号化コンテンツおよび暗号化コンテンツ鍵
802

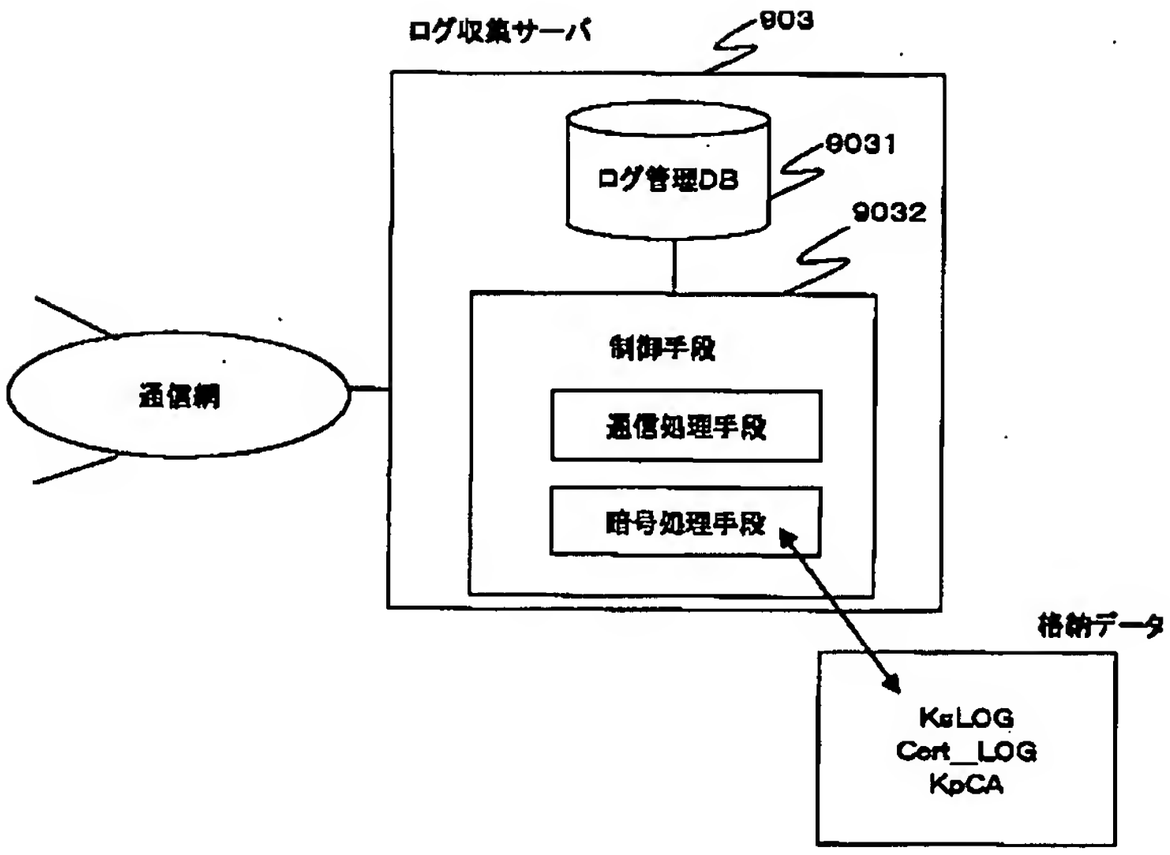
【図５４】


A1～A6:購入処理
B1～B10:ログ送信、証明書更新処理
C1～C5:コンテンツ販売準備処理
D1～D2:売上げ確認処理
906
認証局(CA)
B8. 証明書生成
B7. 証明書依頼
B9. 公開鍵証明書
906
コンテンツプロバイダ
KeCP
Cert_CP
KpCA
C1. コンテンツ生成
D1. 売上げ確認要求
D2. 売上げ回答
903
ログ収集サーバ
KeLOG
Cert_LOG
KpCA
B3. 購入ログ確認
手数料
901
ショップサーバ
KeSHOP
Cert_SHOP
KpCA
手数料
C2. コンテンツ
904
オーサリングサーバ
KeSP
Cert_SP
KpCA
A3. 購入要求確認
A7. 課金
C5. ヘッダ、コンテンツ保存
C4. 1. ヘッダ
C4. 2. コンテンツ
C3. ヘッダ生成、コンテンツ暗号化
B4. 公開鍵要求
A2. 購入要求
A4. 1. 販売確認
A4. 2. ヘッダ
A4. 3. コンテンツ
B2. 購入ログ
A8. 受信確認
B10. 公開鍵証明書
B6. 新しい公開鍵
902
ユーザ機器
KeDEV
Cert_DEV
KpCA
A1. 購入コンテンツ決定
A5. 販売確認、ヘッダコンテンツ受信
A8. 購入ログ生成、保存
B1. 公開鍵更新要求生成
B5. 鍵ペア生成
B11. 証明書受信、保存

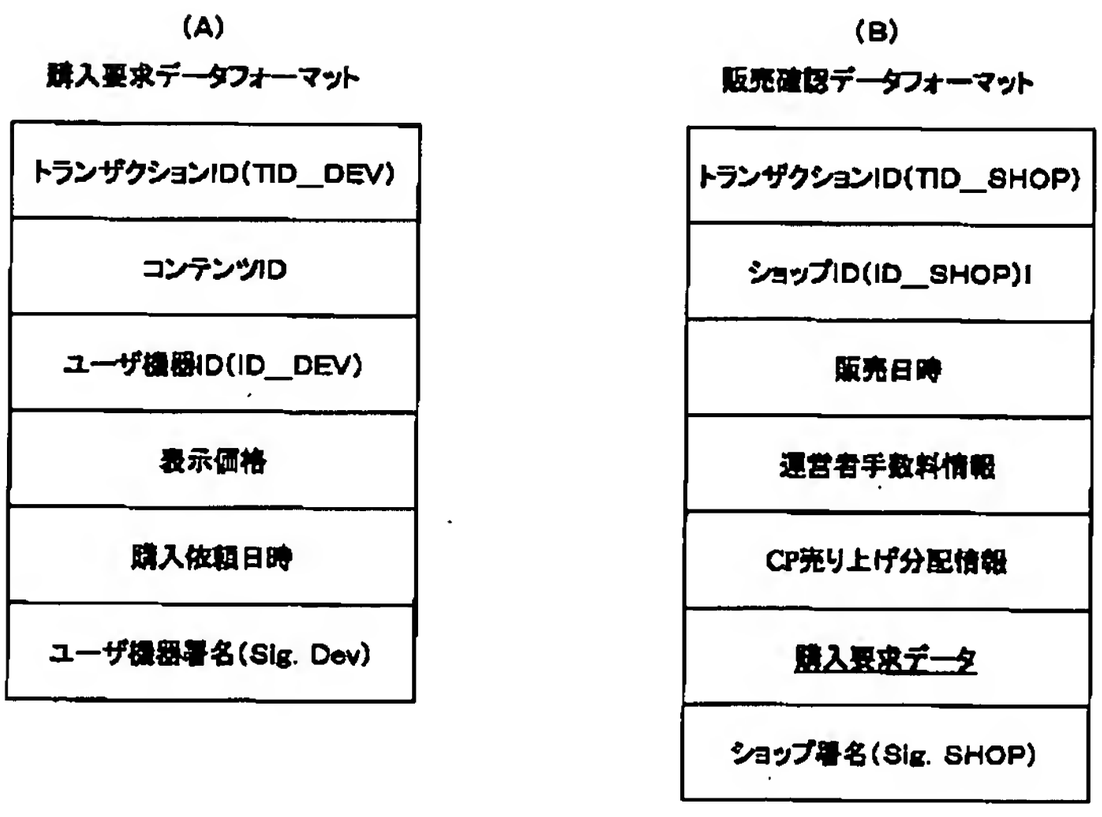
【図５５】


(A)
構成例1
コンテンツID
ユーザ機器ID(ID_DEV)
ショップID(ID_SHOP)I
日付情報
ユーザ機器署名(Sig. Dev)
(B)
構成例2
販売確認データ
受け取り日時
ユーザ機器署名(Sig. Dev)

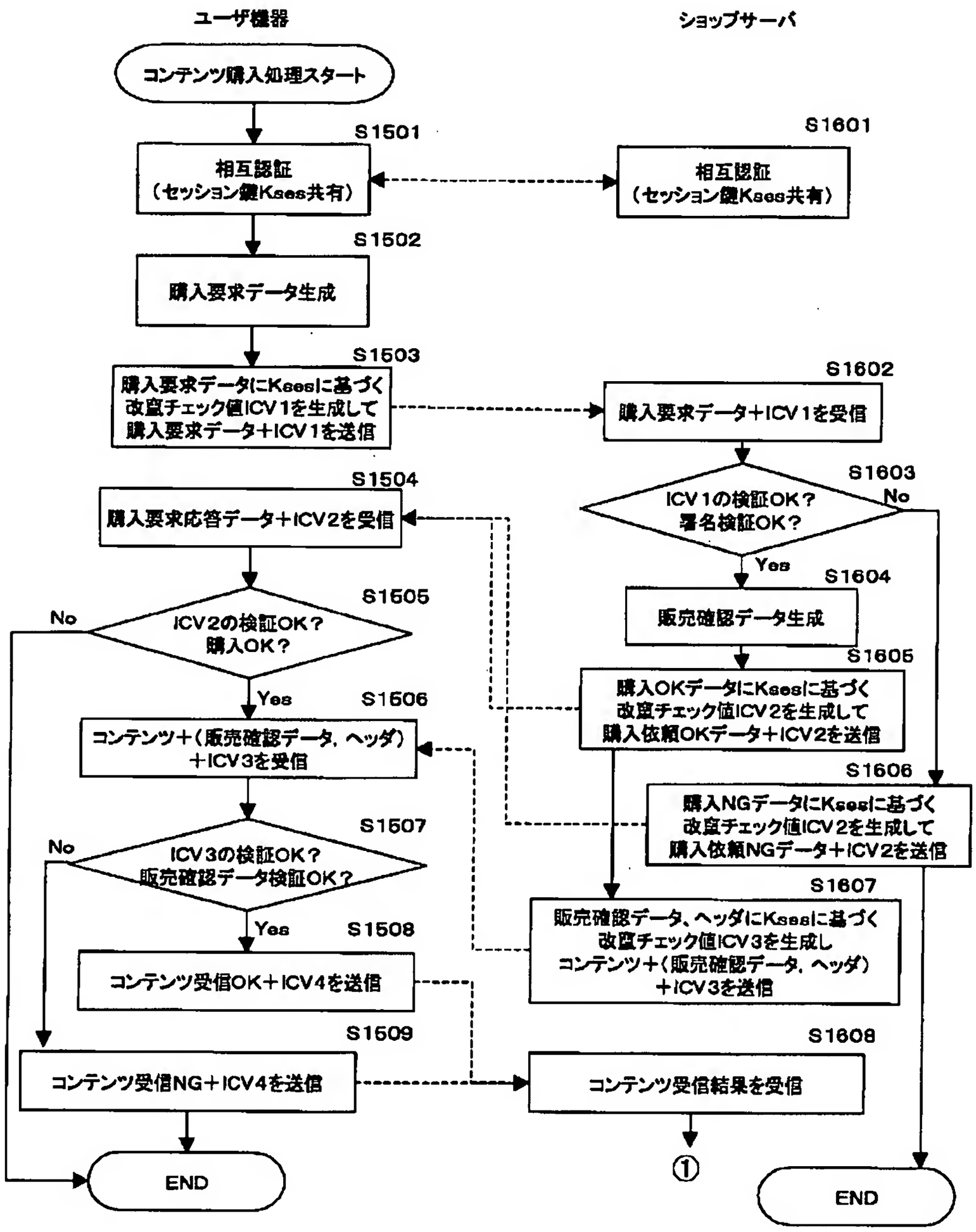
【図５６】


ログ収集サーバ
903
ログ管理DB
9031
9032
制御手段
通信網
通信処理手段
暗号処理手段
格納データ
KgLOG
Cert_LOG
KpCA

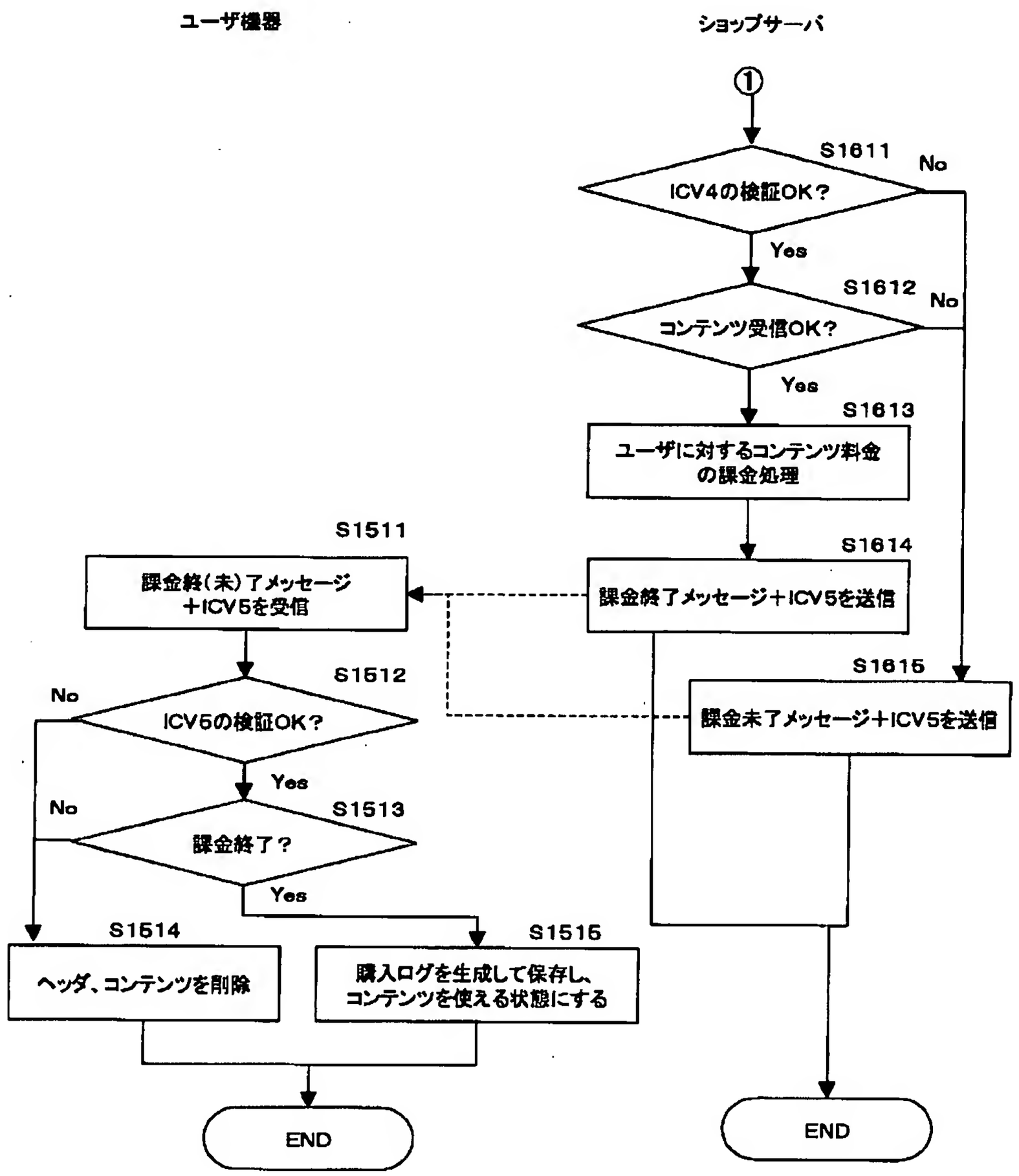
【図５９】


(A)
購入要求データフォーマット
トランザクションID(TID_DEV)
コンテンツID
ユーザ機器ID(ID_DEV)
表示価格
購入依頼日時
ユーザ機器署名(Sig. Dev)
(B)
販売確認データフォーマット
トランザクションID(TID_SHOP)
ショップID(ID_SHOP)I
販売日時
運営者手数料情報
CP売り上げ分配情報
購入要求データ
ショップ署名(Sig. SHOP)

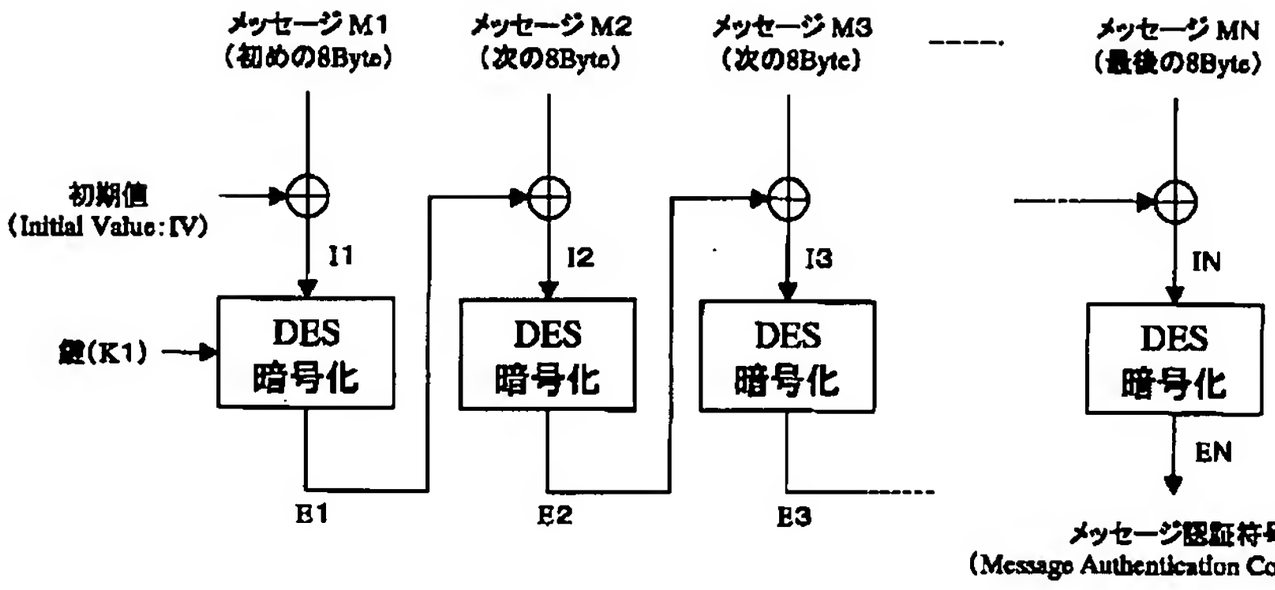
【図５７】


ユーザ機器
ショップサーバ
コンテンツ購入処理スタート
S1501
相互認証
（セッション鍵Kses共有）
S1601
相互認証
（セッション鍵Kses共有）
S1502
購入要求データ生成
S1503
購入要求データにKsesに基づく
改竄チェック値ICV1を生成して
購入要求データ+ICV1を送信
S1602
購入要求データ+ICV1を受信
S1603
ICV1の検証OK？
署名検証OK？
No
Yes
S1504
購入要求応答データ+ICV2を受信
S1604
販売確認データ生成
S1505
No
ICV2の検証OK？
購入OK？
Yes
S1605
購入OKデータにKsesに基づく
改竄チェック値ICV2を生成して
購入依頼OKデータ+ICV2を送信
S1606
購入NGデータにKsesに基づく
改竄チェック値ICV2を生成して
購入依頼NGデータ+ICV2を送信
S1506
コンテンツ+（販売確認データ，ヘッダ）
+ICV3を受信
S1507
No
ICV3の検証OK？
販売確認データ検証OK？
Yes
S1607
販売確認データ、ヘッダにKsesに基づく
改竄チェック値ICV3を生成し
コンテンツ+（販売確認データ，ヘッダ）
+ICV3を送信
S1508
コンテンツ受信OK+ICV4を送信
S1609
コンテンツ受信NG+ICV4を送信
S1608
コンテンツ受信結果を受信
①
END
END

【図５８】

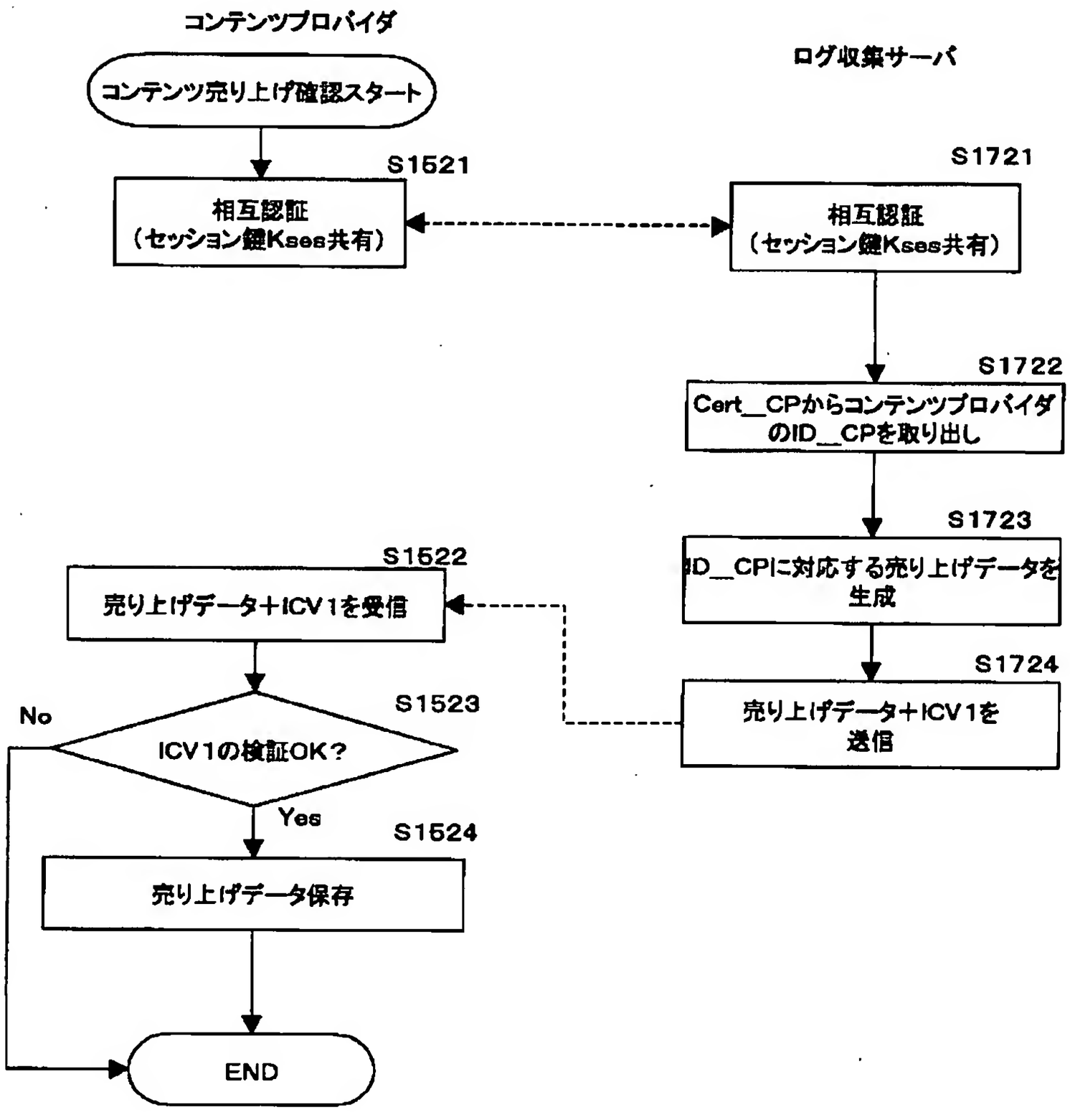

ユーザ機器
ショップサーバ
①
S1611
ICV4の検証OK？
No
Yes
S1612
コンテンツ受信OK？
No
Yes
S1613
ユーザに対するコンテンツ料金の課金処理
S1614
課金終了メッセージ＋ICV5を送信
S1615
課金未了メッセージ＋ICV5を送信
S1511
課金終(未)了メッセージ＋ICV5を受信
S1512
ICV5の検証OK？
No
Yes
S1513
課金終了？
No
Yes
S1514
ヘッダ、コンテンツを削除
S1515
購入ログを生成して保存し、コンテンツを使える状態にする
END
END

【図６０】

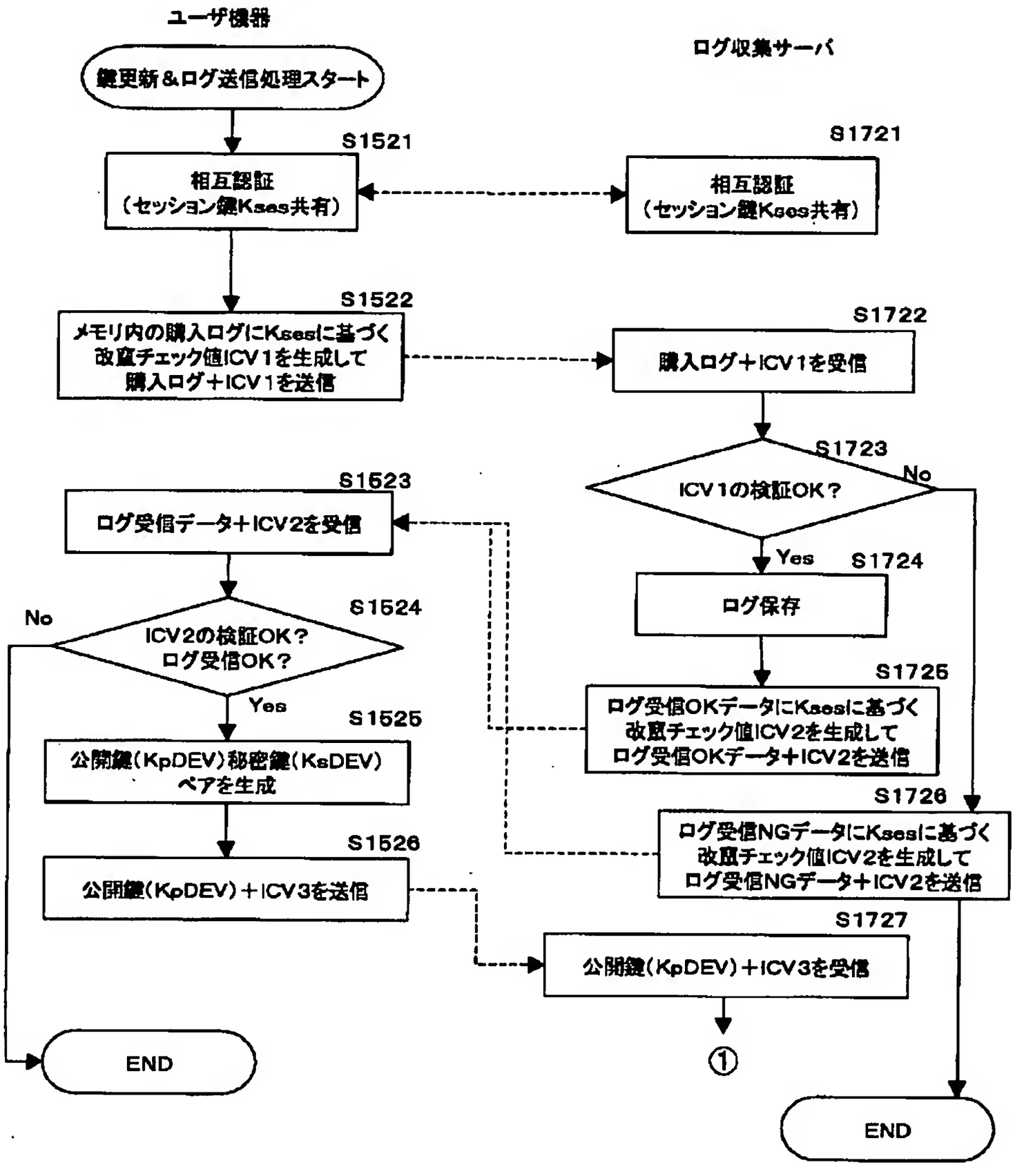


⊕ :排他的論理和処理(8バイト単位)

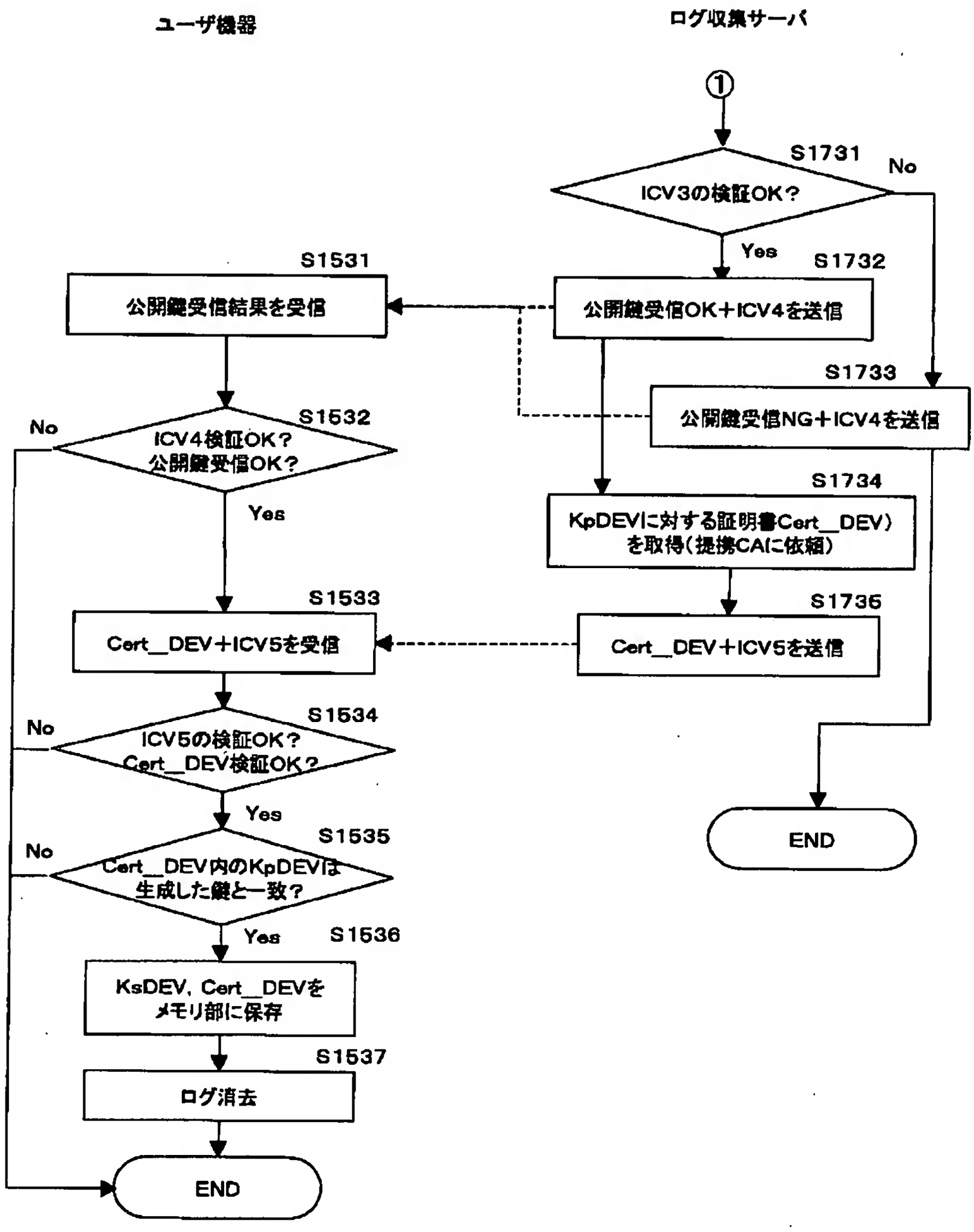
【図６３】



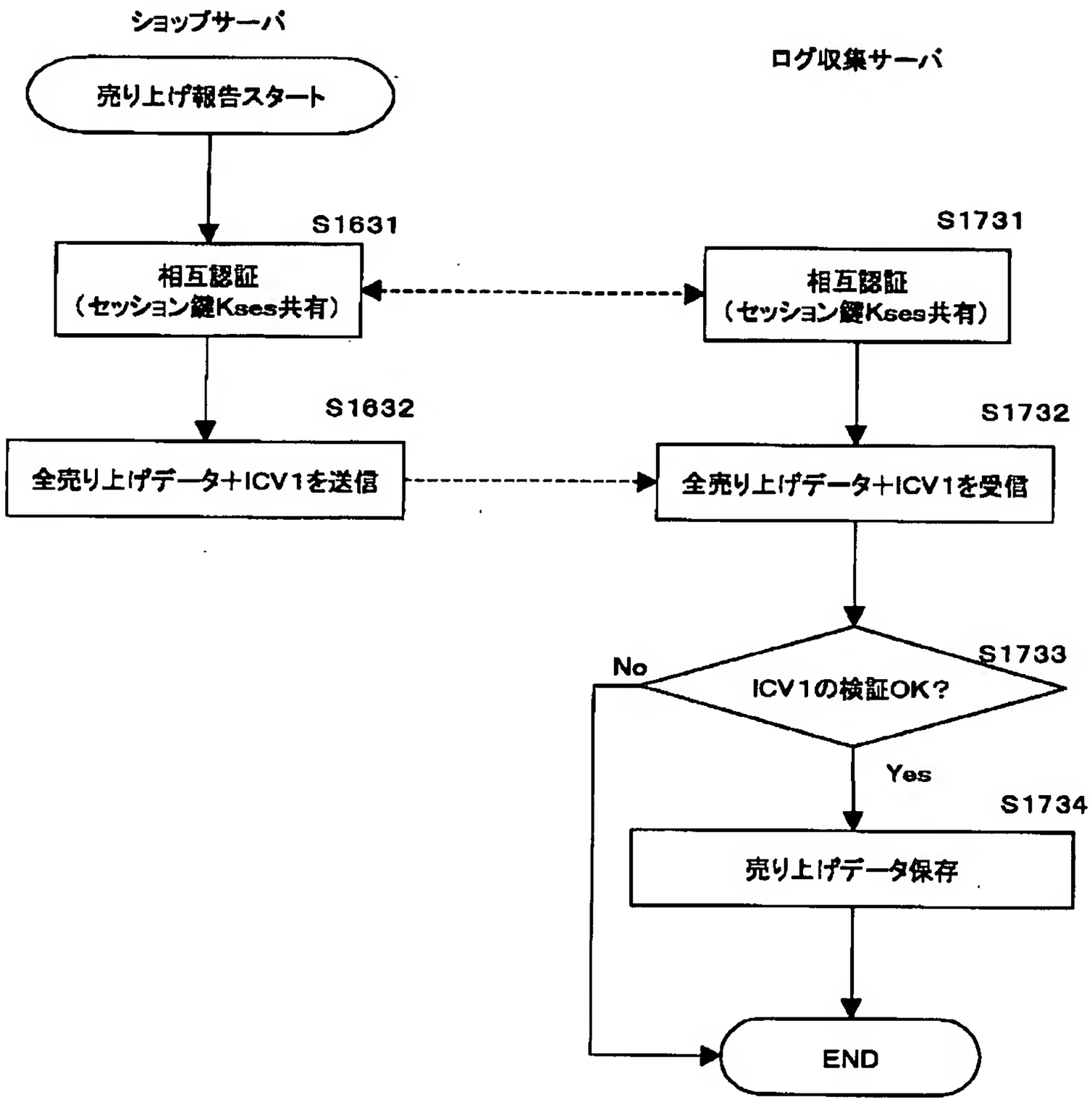
【図６１】


ユーザ機器
ログ収集サーバ
鍵更新＆ログ送信処理スタート
S1521
相互認証
（セッション鍵Kses共有）
S1721
相互認証
（セッション鍵Kses共有）
S1522
メモリ内の購入ログにKsesに基づく
改竄チェック値ICV1を生成して
購入ログ＋ICV1を送信
S1722
購入ログ＋ICV1を受信
S1723
ICV1の検証OK？
No
Yes
S1724
ログ保存
S1725
ログ受信OKデータにKsesに基づく
改竄チェック値ICV2を生成して
ログ受信OKデータ＋ICV2を送信
S1726
ログ受信NGデータにKsesに基づく
改竄チェック値ICV2を生成して
ログ受信NGデータ＋ICV2を送信
S1727
公開鍵（KpDEV）＋ICV3を受信
①
END
S1523
ログ受信データ＋ICV2を受信
S1524
ICV2の検証OK？
ログ受信OK？
No
Yes
S1525
公開鍵（KpDEV）秘密鍵（KsDEV）
ペアを生成
S1526
公開鍵（KpDEV）＋ICV3を送信
END

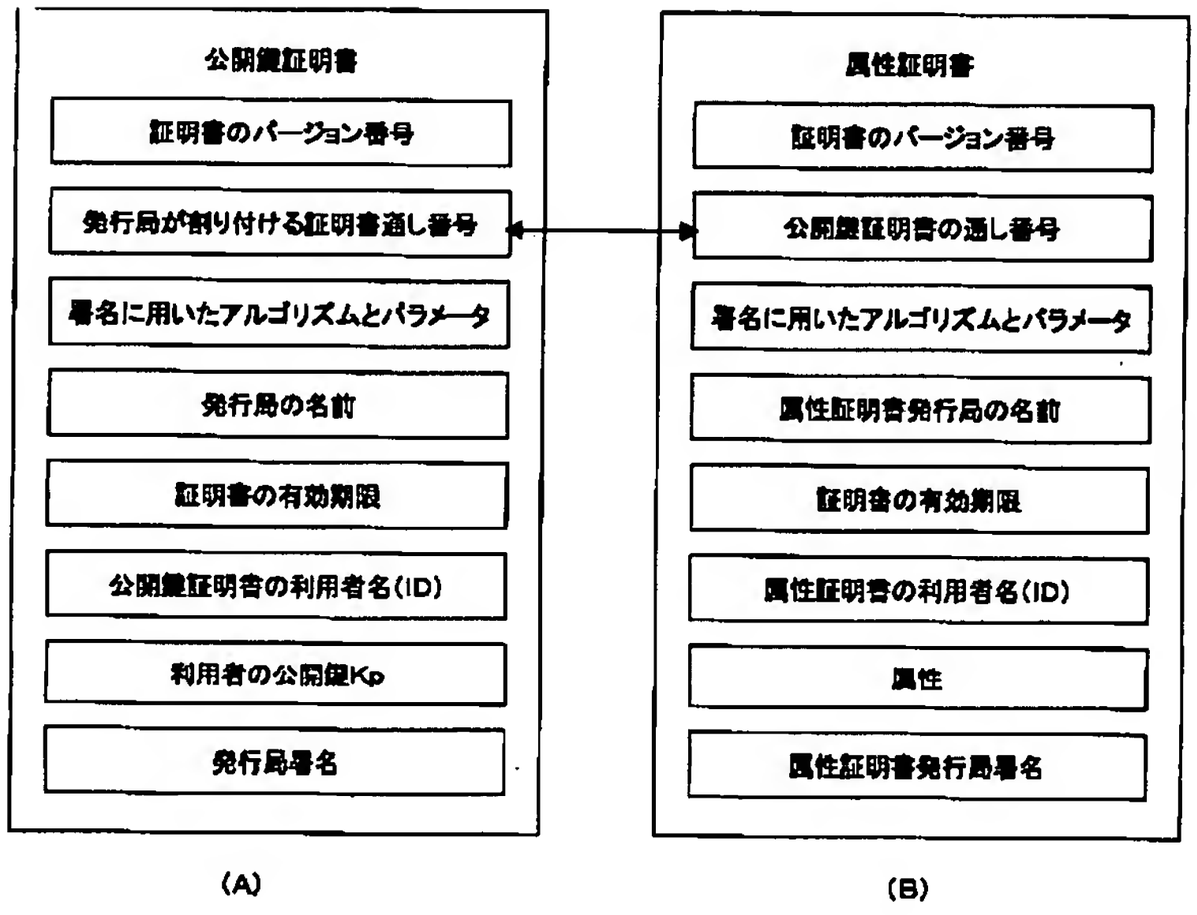
【図６２】


ユーザ機器
ログ収集サーバ
①
S1731
ICV3の検証OK？
No
Yes
S1732
公開鍵受信OK＋ICV4を送信
S1733
公開鍵受信NG＋ICV4を送信
S1734
KpDEVに対する証明書Cert_DEV）
を取得（提携CAに依頼）
S1735
Cert_DEV＋ICV5を送信
END
S1531
公開鍵受信結果を受信
S1532
ICV4検証OK？
公開鍵受信OK？
No
Yes
S1533
Cert_DEV＋ICV5を受信
S1534
ICV5の検証OK？
Cert_DEV検証OK？
No
Yes
S1535
Cert_DEV内のKpDEVは
生成した鍵と一致？
No
Yes
S1536
KsDEV、Cert_DEVを
メモリ部に保存
S1537
ログ消去
END

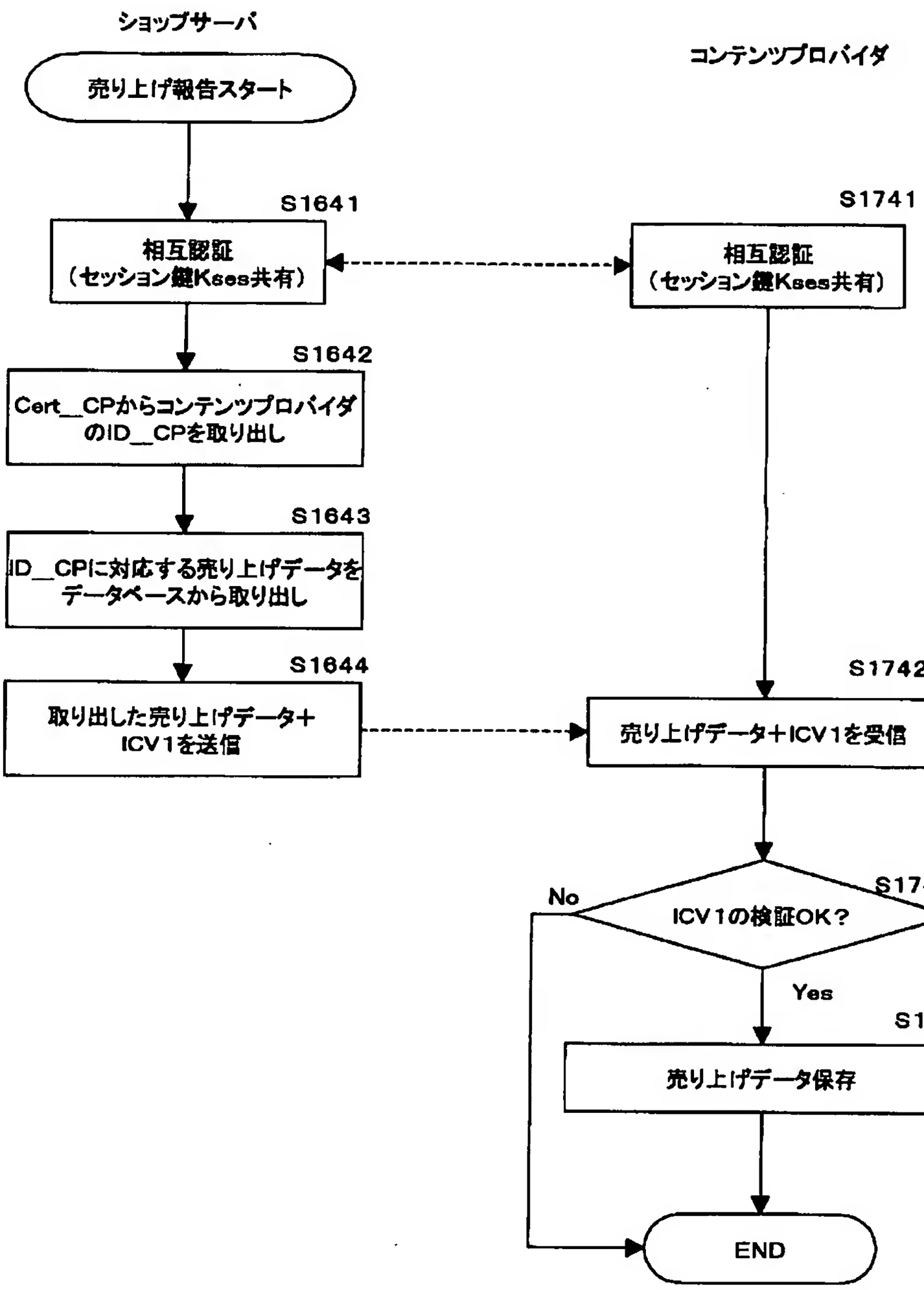
【図６４】


ショップサーバ
ログ収集サーバ
売り上げ報告スタート
S1631
相互認証
（セッション鍵Kses共有）
S1731
相互認証
（セッション鍵Kses共有）
S1632
全売り上げデータ＋ICV1を送信
S1732
全売り上げデータ＋ICV1を受信
S1733
No
ICV1の検証OK？
Yes
S1734
売り上げデータ保存
END

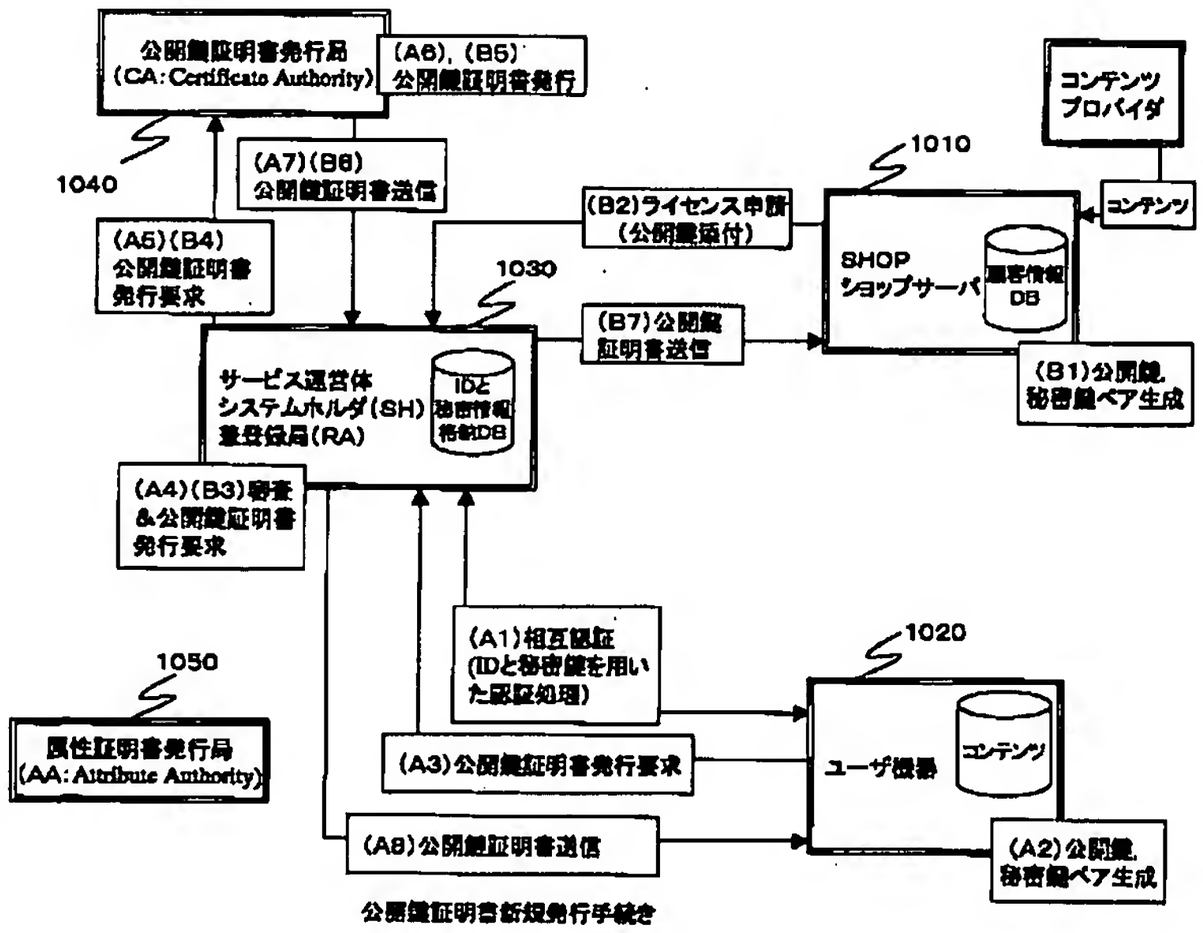
【図６８】


公開鍵証明書
証明書のバージョン番号
発行局が割り付ける証明書通し番号
署名に用いたアルゴリズムとパラメータ
発行局の名前
証明書の有効期限
公開鍵証明書の利用者名(ID)
利用者の公開鍵Kp
発行局署名
(A)
属性証明書
証明書のバージョン番号
公開鍵証明書の通し番号
署名に用いたアルゴリズムとパラメータ
属性証明書発行局の名前
証明書の有効期限
属性証明書の利用者名(ID)
属性
属性証明書発行局署名
(B)

【図６５】

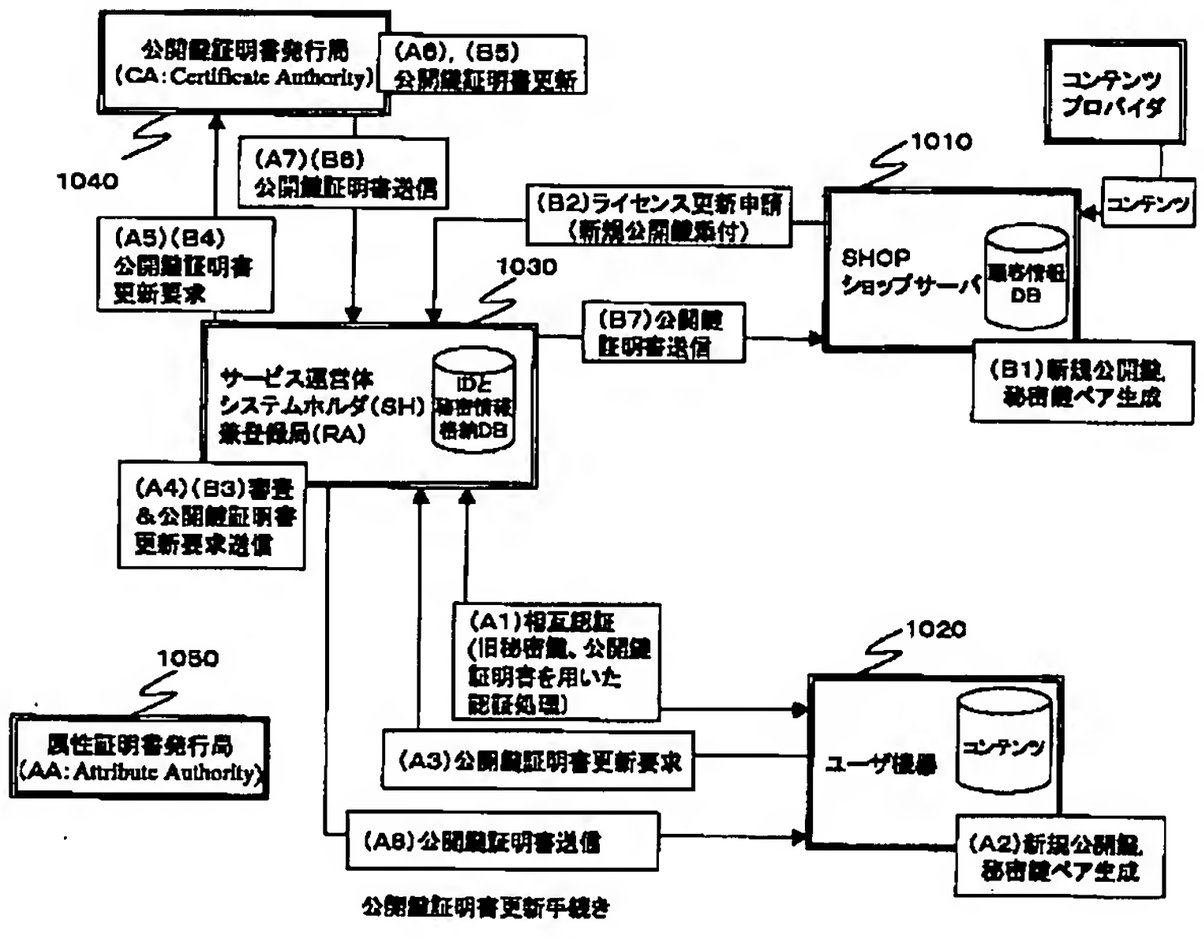

ショップサーバ
コンテンツプロバイダ
売り上げ報告スタート
S1641
相互認証
（セッション鍵Kses共有）
S1741
相互認証
（セッション鍵Kses共有）
S1642
Cert_CPからコンテンツプロバイダ
のID_CPを取り出し
S1643
ID_CPに対応する売り上げデータを
データベースから取り出し
S1644
取り出した売り上げデータ＋
ICV1を送信
S1742
売り上げデータ＋ICV1を受信
S1743
ICV1の検証OK？
No
Yes
S1744
売り上げデータ保存
END

【図６９】



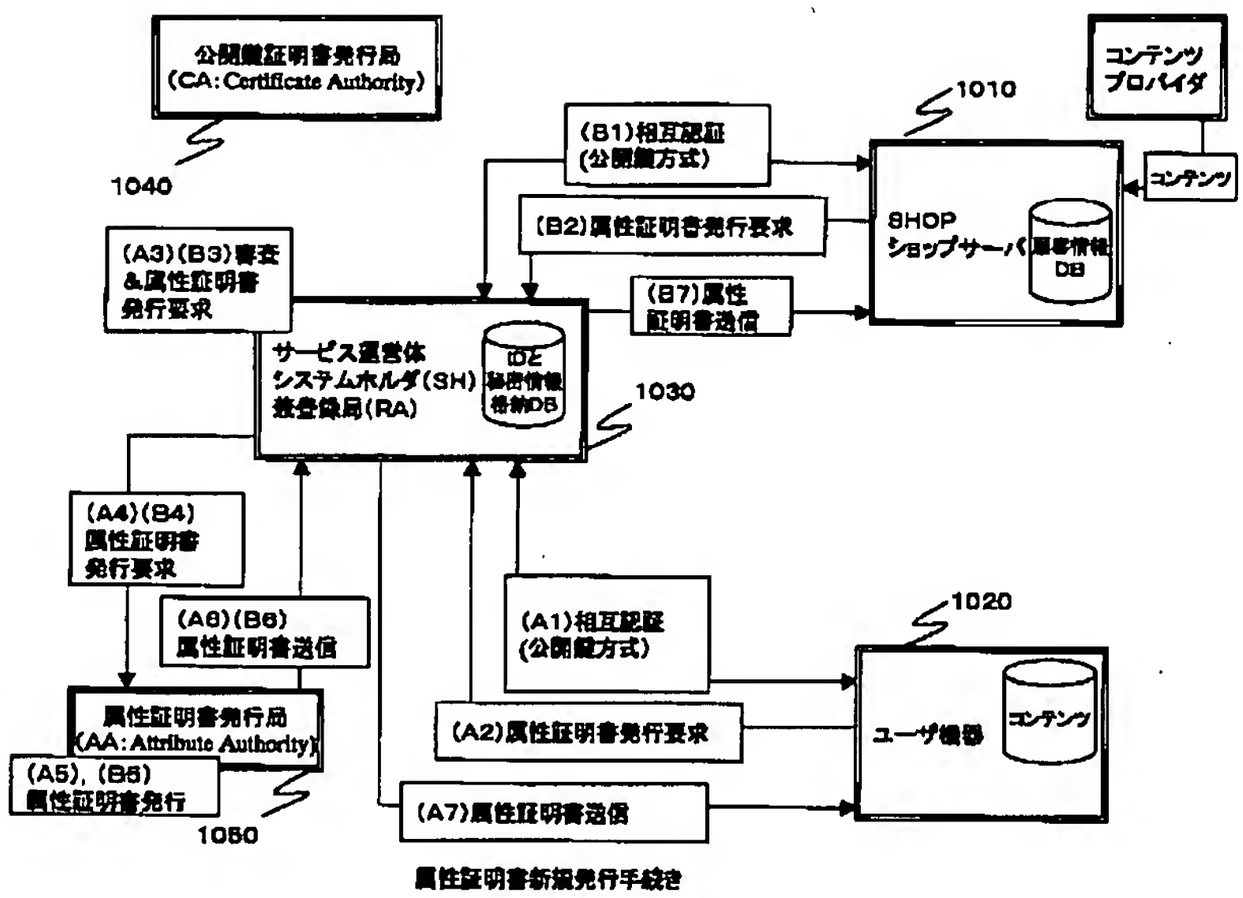
公開鍵証明書新規発行手続き

【図７０】

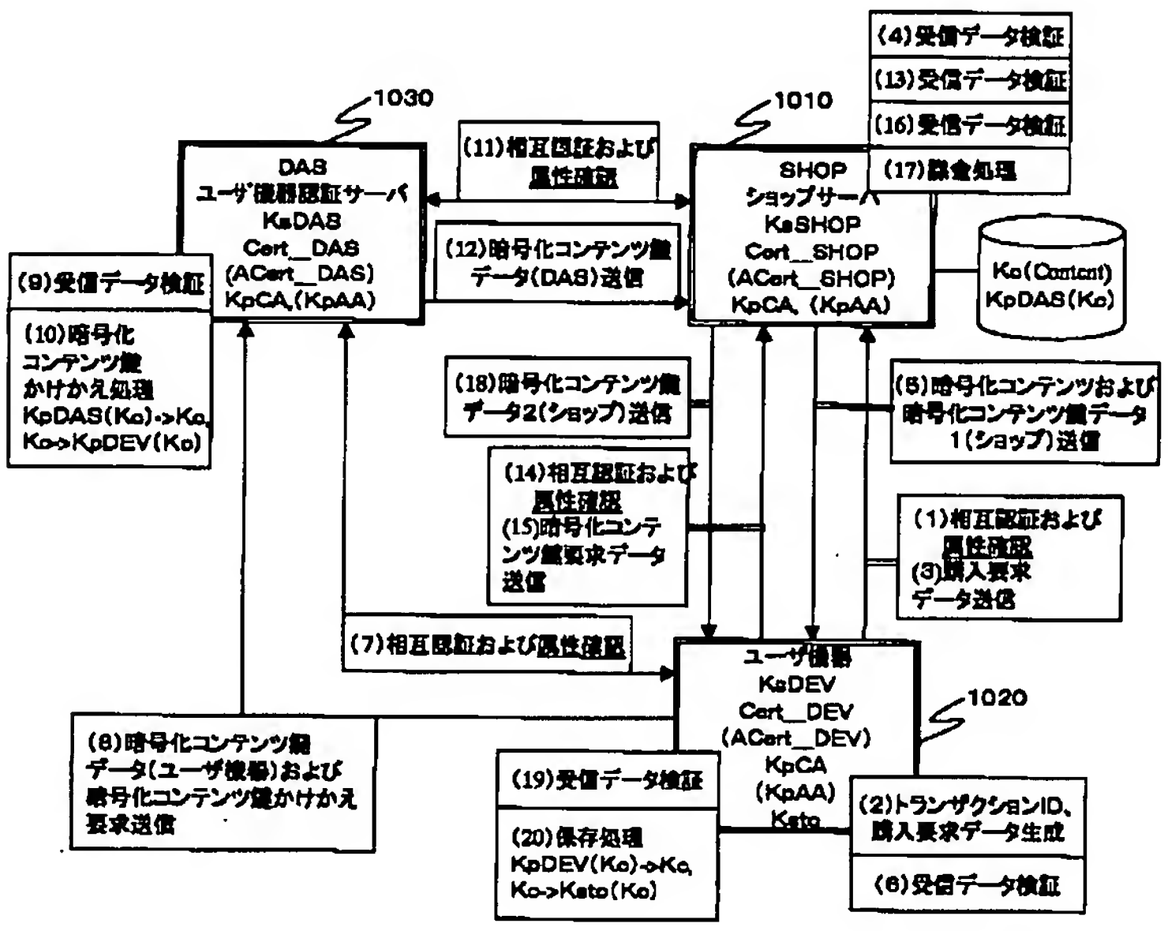


公開鍵証明書更新手続き

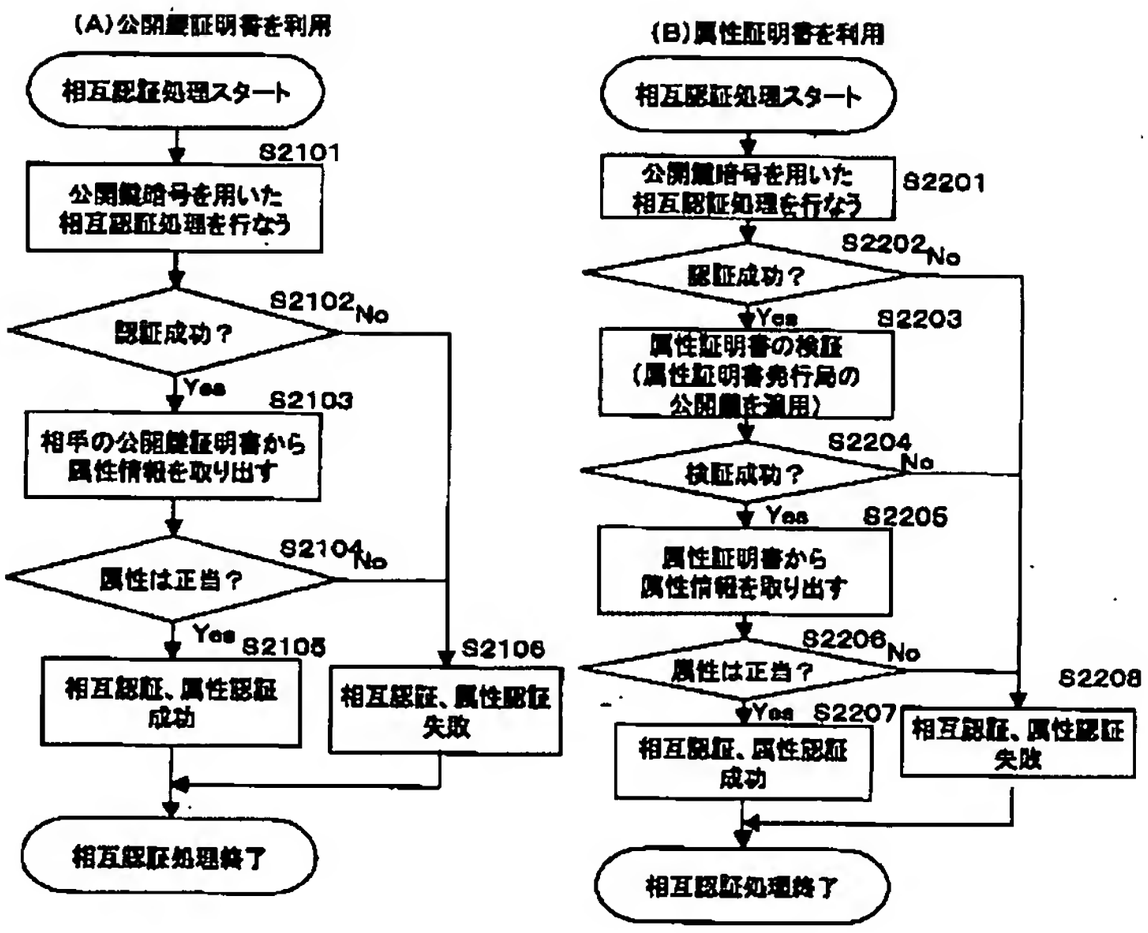
【図７１】


公開鍵証明書発行局
(CA:Certificate Authority)
1040
コンテンツ
プロバイダ
1010
(B1)相互認証
(公開鍵方式)
(B2)属性証明書発行要求
(B7)属性
証明書送信
SHOP
ショップサーバ
コンテンツ
(A3)(B3)審査
&属性証明書
発行要求
サービス運営体
システムホルダ(SH)
登録局(RA)
1030
(A4)(B4)
属性証明書
発行要求
(A6)(B6)
属性証明書送信
(A1)相互認証
(公開鍵方式)
1020
(A2)属性証明書発行要求
ユーザ機器
コンテンツ
属性証明書発行局
(AA:Attribute Authority)
(A5),(B5)
属性証明書発行
1050
(A7)属性証明書送信
属性証明書新規発行手続き

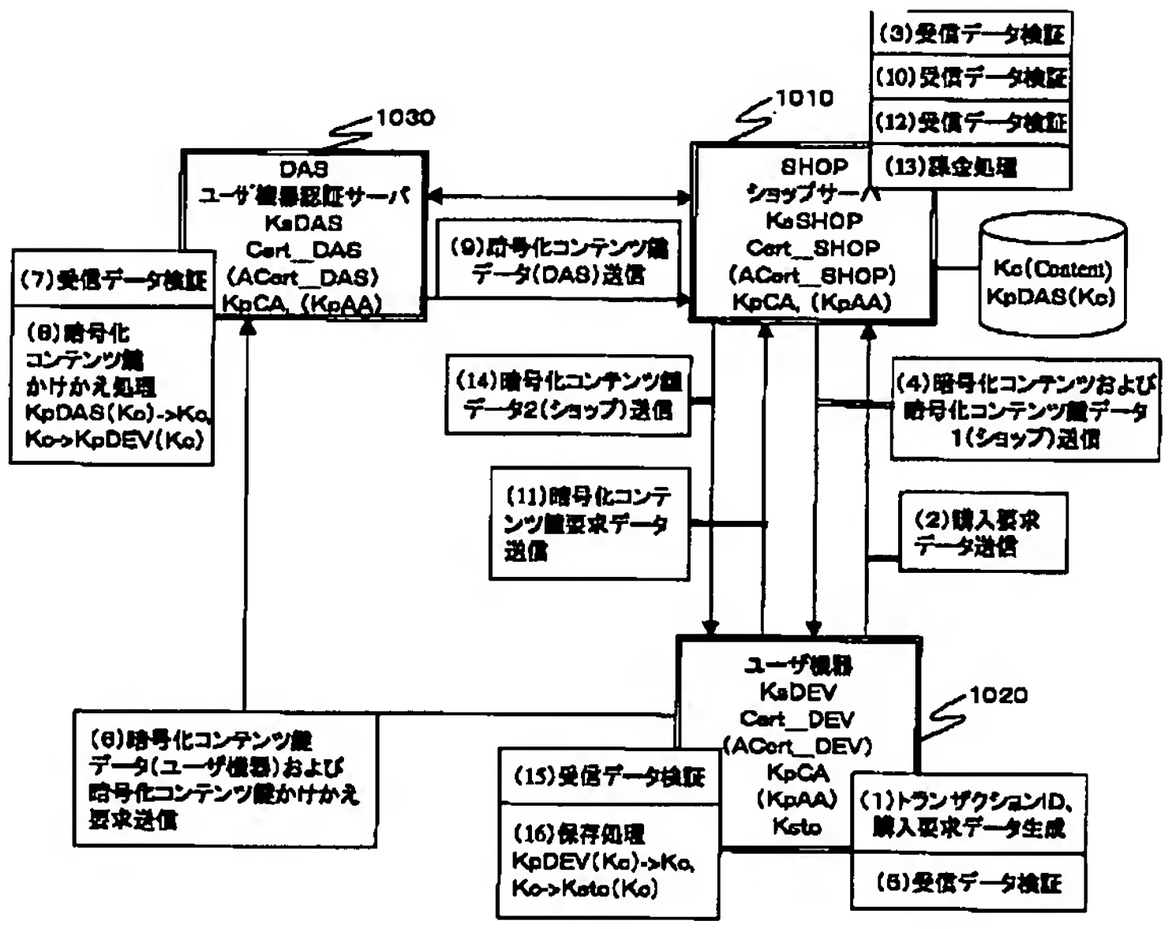
【図７２】


(4)受信データ検証
(13)受信データ検証
(16)受信データ検証
(17)課金処理
1030
1010
(11)相互認証および
属性確認
DAS
ユーザ機器認証サーバ
KsDAS
Cert_DAS
(ACert_DAS)
KpCA,(KpAA)
SHOP
ショップサーバ
KsSHOP
Cert_SHOP
(ACert_SHOP)
KpCA, (KpAA)
(12)暗号化コンテンツ鍵
データ(DAS)送信
Ko(Content)
KpDAS(Ko)
(9)受信データ検証
(10)暗号化
コンテンツ鍵
かけかえ処理
KpDAS(Ko)->Ko,
Ko->KpDEV(Ko)
(18)暗号化コンテンツ鍵
データ2(ショップ)送信
(5)暗号化コンテンツおよび
暗号化コンテンツ鍵データ
1(ショップ)送信
(14)相互認証および
属性確認
(15)暗号化コンテン
ツ鍵要求データ
送信
(1)相互認証および
属性確認
(3)購入要求
データ送信
(7)相互認証および属性確認
ユーザ機器
KsDEV
Cert_DEV
(ACert_DEV)
KpCA
(KpAA)
Ksto
1020
(8)暗号化コンテンツ鍵
データ(ユーザ機器)および
暗号化コンテンツ鍵かけかえ
要求送信
(19)受信データ検証
(20)保存処理
KpDEV(Ko)->Ko,
Ko->Ksto(Ko)
(2)トランザクションID、
購入要求データ生成
(6)受信データ検証

【図７３】



【図７４】



フロントページの続き

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	17/60	５１２	Ｇ０９Ｃ	1/00	６４０Ｂ
Ｇ０９Ｃ	1/00	６４０			６４０Ｚ
			Ｈ０４Ｎ	7/173	６４０Ｚ
Ｈ０４Ｌ	9/32		Ｈ０４Ｌ	9/00	６０１Ｂ
Ｈ０４Ｎ	7/167				６７５Ｄ
	7/173	６４０	Ｈ０４Ｎ	7/167	Ｚ

(72)発明者　石橋　義人
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　秋下　徹
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　白井　太三
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　岡　誠
東京都品川区北品川６丁目７番35号　ソニー株式会社内
(72)発明者　吉森　正治
東京都港区赤坂七丁目１番１号　株式会社ソニー・コンピュータエンタテインメント内

Ｆターム(参考)　5B085 AE09 AE29
5C064 BA07 BB01 BB02 BB07 BC01 BC06 BC17 BC22 BD02 BD04 BD09 BD13 CA14 CB01 CC04
5J104 AA01 AA07 AA16 EA06 EA17 KA01 KA05 MA01 NA02 PA07